Chapter 3 - Report Security

Overview

In this chapter, we see how security domains and security groups control access to reports and report data. We also learn to share custom reports with authorized users and troubleshoot report access issues.

Objectives

By the end of this chapter, you should be able to:

- Describe the security features that control access to reports and report fields.
- Share a report with other users.
- Troubleshoot report access issues.

Scenario

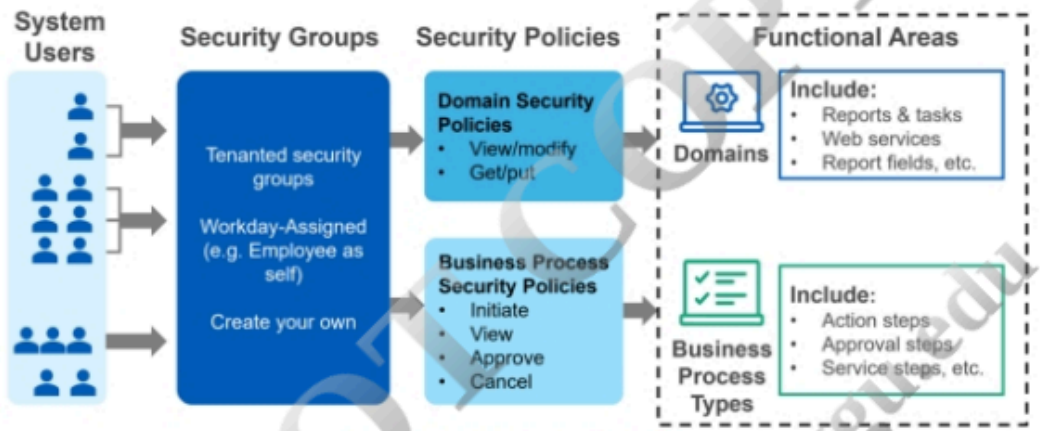
Logan McNeil needs to share an employee audit report with managers.

Employee	Supervisory Organization	Total Base Pay Annualized in USD - Amount	Hire Date	SSN	Age	Emergency Contacts
Nathan Moore	Accounts Payable	85,692.03	01/01/2000	342-10-2843	42	Alice Moore Robert Moore
Jerome Williams	Accounts Payable	80,832.55	01/01/2000	344-20-0127	37	James Williams Ruth Williams
Ian Murray	Accounts Payable	58,349.50	02/01/2013	567-34-9819	28	Samantha Murray

Important: Beth Liu is the manager of the Payroll Department and the payroll administrator for the tenant, which gives her additional access to certain data. Jack Taylor is the manager of the IT Helpdesk Department. They both need to run the report and determine which reports fields and data they can access.

Workday Security Model

The Workday security model controls access to reports and report data.



How security controls access for users ( )

Term	Definition
Security Domain	• A predefined set of related securable items that include reports, tasks, report fields, data sources, and data source filters. • The securable items that make up a domain do not change. • Users in the security group can have view or modify access to the securable items.
Security Group	• A collection of users. • Users are given group membership as individual users or by identifying groups of users by attributes. • Attributes may include their position role assignment, or job

	details such as management level or geographic location.
Domain Security Policy	• Controls a user's access to the securable items in the domain. • Each domain has its own domain security policy that controls access to the securable items in the domain. • Users in the security group can have view or modify access to the securable items. **Note**: Domains secure all delivered items (including data sources, report fields, delivered reports, and tasks). To access an item, users must belong to a security group with access to the domain securing the item. The security administrator can configure the domain security policies and add or remove security groups as needed.

This example shows the Worker Data: Active Employees security domain. This security domain contains three securable items:

- Active Employees, a report.
- Employee Talent Analysis, another report.
- All Active Employees, a data source.

The HR Partner security group has one member, Logan McNeil. This security group identifies users with positions assigned to the HR Partner role.

In this example, Logan can:

- Run the Active Employees and Employee Talent Analysis reports.
- Run a report that uses the All Active Employees data source.

The following table shows examples of using security domains and permitted security groups to control access to reports, tasks, data sources, and report fields.

Securable Item	Security Domain	Permitted Security Groups	Impact
Standard Report: Find Journal Lines	Process: Journals	Accountant Accounting Manager Company Financial Analyst Controller Finance Auditor Financial Management System Implementers	Members of these security groups can run this standard report.
Task: Create Custom Report	Custom Report Creation	Implementers Manager (Unconstrained) Report Writer Setup Administrator Temporary Report Writer	Members of these security groups can create custom reports.
Data Source: All Customer-Owned Deductions	Set Up: Payroll (Calculations - Payroll Specific)	Implementers Payroll Administrator Payroll Auditor Payroll Calculations Administrator Payroll Partner	Members of these security groups can create and run reports that use this data source (assuming the report is shared with them).

Report Field: Billing Schedule	Process: Billing	Accountant Accounting Manager Billing Specialist Cash Analyst Cash Manager Company Financial Analyst Controller Customer Contract Specialist Customer Contracts System Finance Auditor Implementers Revenue Specialist	Members of these security groups can access this report field and create reports with it.

Unconstrained vs. Constrained Security Groups

A security group can be unconstrained or constrained. Users in an unconstrained security group have access to all data for a given object. Users in a constrained security group have contextual access to a subset of data for a given item. For constrained security groups, a user's access to specific data is controlled either by their individual role or their organization.

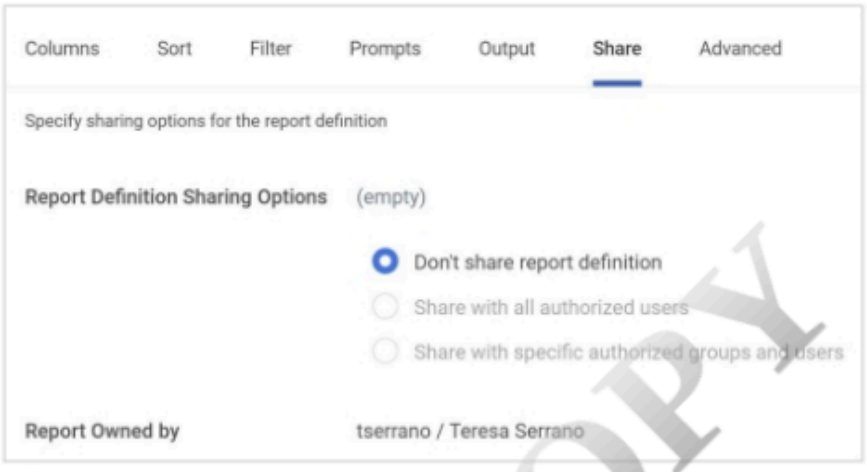
In the following example, Beth Liu is a member of both the Payroll Administrator and Manager security groups. Jack Taylor is a member of the Manager security group. Let us assume that both the Payroll Administrator and Manager security groups have access to the Base Pay Amount report field. Beth sees all data for this report field, since she belongs to an unconstrained security group with access to the report field. Jack only sees his employee's (Jeff Gordon) data for this report field, since he belongs to a constrained security group with access to the report field.

Security Note: A user can be a member of many security groups. A user's access is the union of all their security group access.

User-based and role-based security groups are the most common security group types. User-based security groups are unconstrained security groups manually assigned to users. User-based security groups are often used for administrators that need to see and set up data in the tenant for a given area. Role-based security groups are usually constrained and allow you to identify members based on role-assignment as well as constrain members to target access in organizations assigned to the role.

Sharing Reports

Custom reports are not shared by default. A custom report is visible only to its owner (and to users who have access to manage all custom reports). As shown in the image below, the Share tab lets you share a custom report with authorized users. You can share a custom report with all users who have access to the report data source and data source filter. You can also share a report with specific groups and users who have access to the report data source and data source filter. The domain securing the custom report's data source determines which security groups you can share the custom report with.



Security Note: You can control if report writers can use the different sharing options. Report writers must have access to these security domains to use the sharing options:

- Domain: Report Definition Sharing - All Authorized Users
- Domain: Report Definition Sharing - Specific Groups
- Domain: Report Definition Sharing - Specific Users

When you share a report, users can run the report, but they cannot edit it. Only the report owner (and those who can manage all custom reports) can edit custom reports. However, a shared user can view the report definition and copy the report definition if the shared user is also a report writer.

Note: You can use the Start Proxy task to easily test the report as a shared user. This lets you verify that a user can view the appropriate data in the report.

What Can Users View on a Shared Report?

A user running a shared report can view the report results based on their security to the data source, data source filter, and report fields. The following example shows the report output when Jack Taylor runs a shared report.

Organization IT HelpDesk Department

2 items

Employee	Supervisory Organization	Total Base Pay Annualized in USD - Amount	Hire Date	Social Security Number - Formatted
Jeff Gordon	IT HelpDesk Department	79,889.00	01/01/2000	
Jack Taylor	IT Services Group	171,455.00	01/01/2000	322-04-4822

The Workday security model determines what Jack can view on the report:

- He can only view two instances (rows) based on his access to the data source. Jack can only view employees in his organization (IT HelpDesk Department).
- He cannot view the Social Security number for his employee Jeff Gordon. Jack has constrained access to this report field, so he can only view his own Social Security number.
- He cannot view the Age and Emergency Contacts report fields at all in the output. Jack does not have any access to these report fields.

The following example shows the report output when Logan McNeil runs a shared report. Logan McNeil has unconstrained access to the report.

Organization Global Modern Services, Inc. (USA)

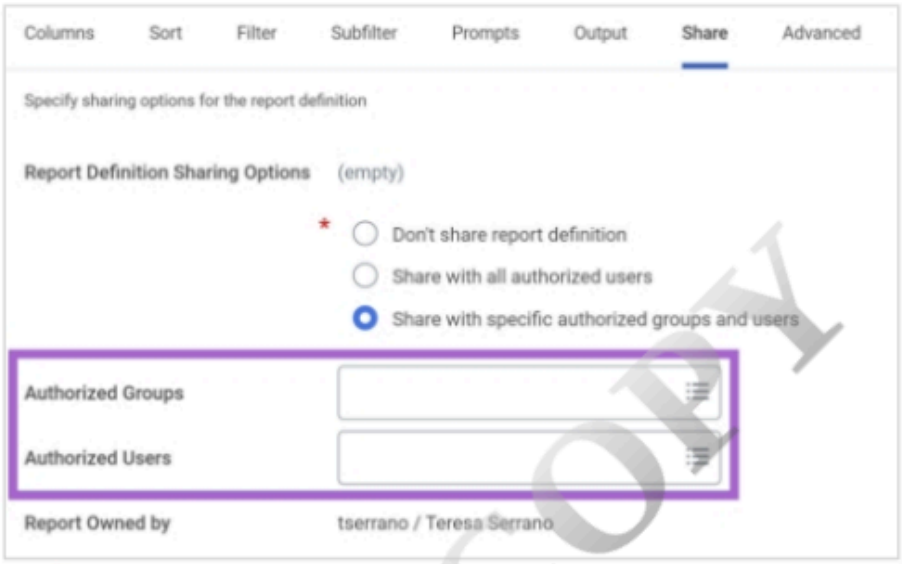
204 items

Employee	Supervisory Organization	Total Base Pay Annualized in USD - Amount	Hire Date	Social Security Number - Formatted	Age	Emergency Contacts
James Walker	Accounting Operations	114,067.00	01/01/2000	342-02-3411	53	Adam Gunderson
Kyle Hopkins	Accounting Operations	149,480.00	01/01/2000	121-04-9418	57	Vanessa Hopkins
Victoria Evans	Accounting Operations	144,536.00	01/01/2000	539-04-1088	54	Lawrence Evans

Data Source and Data Source Filter Security

Security domains contain both report data sources and data source filters. You need to identify which domains contains a data source and data source filter in order to determine if a user has access to report data. Using that information, you can grant the user security access to the necessary domain to display the report data. You can use the View Security for Securable Item report to view the security configurations for any object in the Workday system. This includes data sources and data source filters.

Remember, to share a report with a user, they must have security access to both the report data source and the data source filter used in the report. The "Share with specific authorized groups and users" option prompts you to select which authorized security groups or users you wish to share the report with. Only security groups and users authorized to access both the report's data source and data source filter are selectable from these prompts.



Note: You may receive an error when sharing a report with an allowed security group if you later change the data source filter for the report. This happens when the security groups you have selected do not have access to the newly selected data source filter.

Common Report Access Issues

The following table shows common report access issues that users face when running a shared report.

Issue	Root Cause
A user cannot run a standard report.	The user does not have access to a domain

	securing the standard report.
A user cannot run a custom report.	The custom report is not shared with the user.
Report field data for certain instances does not display.	The data is missing for these instances or the user belongs to a security group that has constrained access to the report field.
A report field does not display at all.	The user does not belong to a security group that has access to the report field.
A different number of instances display for one user compared to another.	The user belongs to a security group that has constrained access to the data source or to report fields used in filters.
A user gets an error that they do not have access to a report field when running a report.	The user does not belong to a security group that has access to a report field used to generate the report, such as in a filter or subfilter.

These are the basic steps you should take when troubleshooting report access issues:

1. Verify that the user should have access to the report or data.
2. Determine which domains secure the standard report, data source, or report field and the permitted security groups.
3. Determine which security groups the user belongs to.
4. Add the user to a security group that already has access to the domain or edit the domain security policy to include a security group to which the user belongs.

You need to work with your security team to view security groups, view security domains, and change the domain security policy. The security team can use these Workday standard reports to troubleshoot report access issues:

Standard Report	Description
View Security for Securable Item	Shows the security policies and permitted security groups for a securable item, such as a data source or report field.
Security Analysis for Securable Item and Account	View the security policies and security groups that grant a

	specified user access to a specified delivered securable item.
View Security Groups for User	Shows which security groups a user belongs to.

Below are the specific steps to take to troubleshoot each report access issue. Remember to first check that the user should have access to the report or data.

Issue - A User Cannot Run a Standard Report

Root Cause	**The user does not have access to a domain securing the standard report.**
Resolution	1. Run the View Security for Securable Item report and enter the name of the report as the item. Find the report name in the resulting matches and select View Security. Here you can review the securing domain(s) and the permitted security groups. 2. Run the View Security Groups for User report to identify which security groups a user belongs to. 3. Add the user to a security group that can already access the domain or edit the domain security policy to include a security group that the user belongs to.

Issue - A User Cannot Run a Custom Report

Root Cause	The custom report is not shared with the user.
Resolution	1. View the Share tab of the custom report definition to review which authorized users and groups the report is shared with. 2. Share the custom report with the user or with a security group that the user belongs to. If the report cannot be shared with the user, then the user does not belong to a security group with access to the custom report's data source or data source filter. 3. Select Security > View Security from the data source's Related Actions to identify the security domains and permitted security groups. (Note: You can also run the View Security for Securable Item report for the data source to get this information.) 4. Run the View Security Groups for User report to identify which security groups a user belongs to. 5. Add the user to a security group that can already access the domain or edit the domain security policy to include a security group that the user belongs to. 6. Share the custom report with the user or with a security group that the user belongs to after configuring security.

Issue - Report Field Data for Certain Instances Does Not Display

Root Cause	The data is missing for these instances or the user belongs to a security group that has constrained access to the report field.
Resolution	1. Have a user with unconstrained access run the report and verify that data exists for these instances. 2. Run the Security Analysis for Securable Item and Account report. Select the report as the Securable Item and select the user. 3. Review which security group gives the user access to the report field. 4. Verify that the security group is constrained and confirm that the data should appear based on this constraint. 5. Edit the domain security policy for the report field to give the user unconstrained access.

Issue - A Report Field Does Not Display at All

Root Cause	The user does not belong to a security group that has access to the report field.
Resolution	1. Select Security > View Security from the report field's Related Actions to identify the security domains and permitted security groups. (Note: You can also run the View Security for Securable Item report for the report field to get this information.) 2. Run the View Security Groups for User report to identify which security groups a user belongs to. 3. Add the user to a security group that can already access the domain or edit the domain security policy to include a security group the user belongs to.

Issue - A Different Number of Instances Display for One User Compared to Another User

Root Cause	**The user belongs to a security group that has constrained access to the data source or to report fields used in filters.**
Resolution	1. Run the View Security Groups for User report to identify which security groups a user belongs to. 2. Select Security > View Security from the data source's Related Actions to identify the security domains and permitted security groups. (Note: You can also run the View Security for Securable Item report for the data source to get this information.) 3. Run the Security Analysis for Securable Item and Account report. Select the report data source as the Securable Item and select the user. 4. Review which security group gives the user access to the data source. 5. Verify that the security group is constrained and confirm that the data should not appear based on this constraint.

Issue - When Running a Report, A User Gets an Error That They Do Not Have Access to a Report Field.

Root Cause	**The user does not belong to a security group that has access to a report field used to generate the report, such as in a filter or subfilter.**
Resolution	1. Read the error message to determine which field is causing the issue. 2. Select Security > View Security from the report field's Related Actions to identify the security domains and permitted security groups. (Note: You can also run the View Security for Securable Item report for the report field to get this information.) 3. Run the View Security Groups for User report to identify which security groups a user belongs to. 4. Add the user to a security group that can already access the domain or edit the domain security policy to include a security group that the user belongs to.

Who Can Create, Edit, Copy, and Delete a Custom Report?

Users with access to the Custom Report Creation security domain can create a custom report. Security domains control access to data sources and report fields. When creating a custom report, you must have view permissions for:

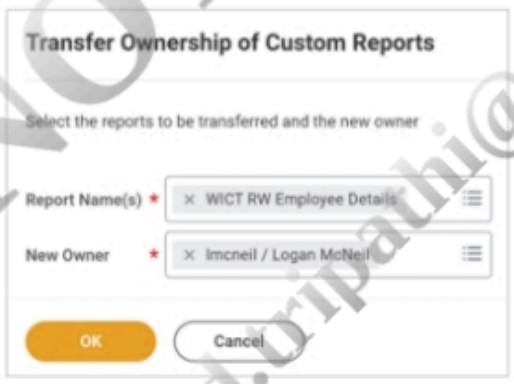
- A security domain for the data source you want to use.
- Security domains for the report fields you want to add.

Prompts only show the data sources and report fields you have access to.

The report owner and users with modify access to the Manage: All Custom Reports security domain can edit and delete a custom report. You cannot delete a custom report definition in use anywhere, such as a worklet on a dashboard.

Transfer Ownership of a Report

You can use the Transfer Ownership of Custom Reports task to change the owner of one or more reports to a different user. This task is useful when people leave the company or change jobs. The new owner must have access to the report's data source and data source filter and have access to the Custom Report Creation security domain.



Security Note: You must have access to the Custom Report Administration or Manage: All Custom Reports security domain to transfer ownership of reports owned by other users. While you can transfer ownership without granting access to the fields in the report definition, the new owner cannot save changes to the report without access to all fields in the report definition.

Custom Report Exception Audit

Run the Custom Report Exception Audit standard report to view warnings and errors for custom reports. This report is helpful when transferring ownership of a report to another user. You can transfer a report to another user as long the new owner has access to the data source. However, an error will appear if the new owner tries to edit the custom report without access to all of the report fields. Running this report can identify these errors ahead of time.

Chapter Summary

Key Takeaways:

- Security domains control access to standard reports, data sources, and report fields.
- A domain security policy links a security group to a security domain.
- You need access to the Custom Report Creation security domain, the data source, and the report fields to create a custom report.
- Users running a shared report see the report results based on their security.

Resources:

- View Security for Securable Item report
- View Security Groups for User report
- Transfer Ownership of Custom Reports task

Chapter Knowledge Check

1. What groups securable items like reports, fields, and data sources?
   a. Security Domain
   b. Domain Security Policy
   c. Security Group
   d. Share Tab on Report

2. A user runs an employee report that includes the Citizenship Status field. The Citizenship Status field appears for some employees, but not all. What is the root cause?
   a. The user has unconstrained access to the Citizenship Status field.
   b. A filter has been added to limit the instances returned.
   c. The user has constrained access to the Citizenship Status field.
   d. A sort has been applied.