

Lab instructions

Enforce model security

Overview

The estimated time to complete the lab is 45 minutes

In this lab, you will update a pre-developed data model to enforce security. Specifically, salespeople at the Adventure Works company should only be able to see sales data related to their assigned sales region.

In this lab, you learn how to:

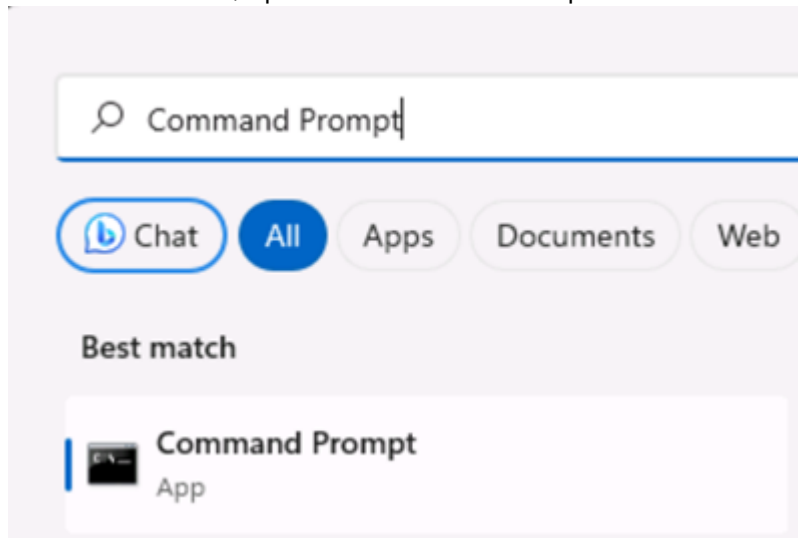
- Create static roles.
- Create dynamic roles.
- Validate roles.
- Map security principals to dataset roles.

Get started

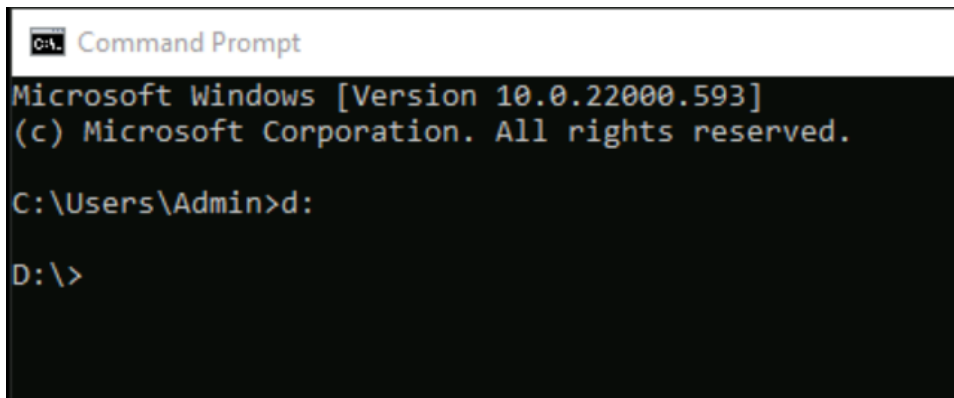
In this exercise, you will prepare your environment.

Clone the repository for this course

1. On the start menu, open the Command Prompt



2. In the command prompt window, navigate to the D drive by typing:
d:
Press enter.



```
Command Prompt
Microsoft Windows [Version 10.0.22000.593]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>d:

D:\>
```

3. In the command prompt window, enter the following command to download the course files and save them to a folder called DP500.

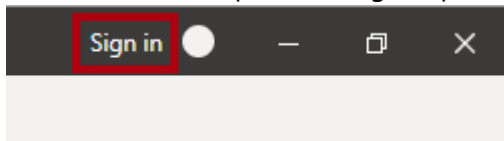
`git clone https://github.com/MicrosoftLearning/DP-500-Azure-Data-Analyst DP500`

4. When the repository has been cloned, close the command prompt window.
5. Open the D drive in the file explorer to ensure the files have been downloaded.

Set up Power BI Desktop

In this task, you will set up Power BI Desktop.

6. To open File Explorer, on the taskbar, select the **File Explorer** shortcut.
7. Go to the **D:\DP500\Allfiles\09\Starter** folder.
8. To open a pre-developed Power BI Desktop file, double-click the **Sales Analysis - Enforce model security.pbix** file.
9. If you're not already signed in, at the top-right corner of Power BI Desktop, select **Sign In**. Use the lab credentials to complete the sign in process.



10. To save the file, on the **File** ribbon, select **Save as**.
11. In the **Save As** window, go to the **D:\DP500\Allfiles\09\MySolution** folder.
12. Select **Save**.

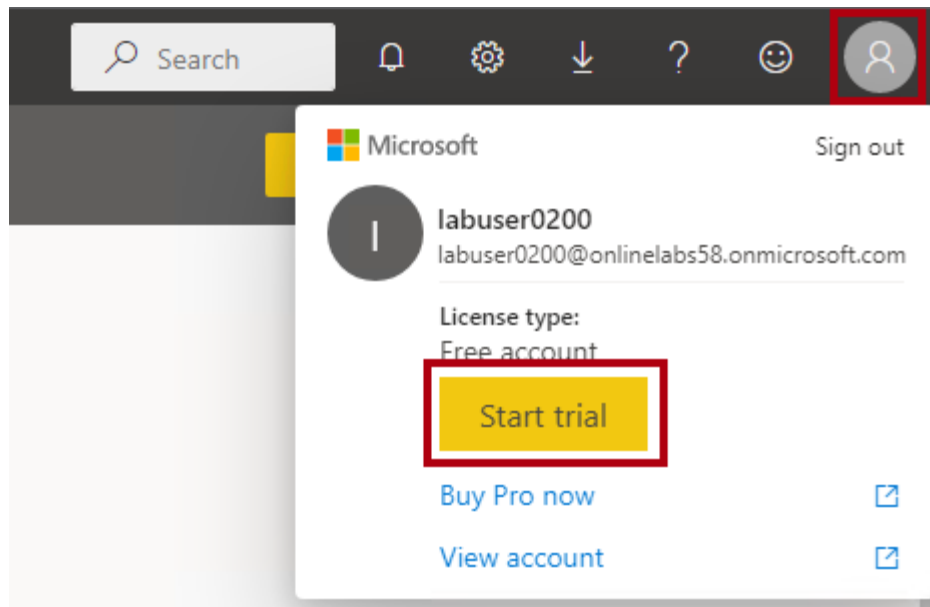
You will update the Power BI Desktop solution to enforce row-level security.

Sign in to the Power BI service

In this task, you will sign in to the Power BI service, start a trial license, and create a workspace.

Important: If you have already setup Power BI in your VM environment, continue to the next task.

13. In a web browser, go to <https://powerbi.com>.
14. Use the lab credentials to complete the sign in process.
Important: You must use the same credentials used to sign in from Power BI Desktop.
15. At the top-right, select the profile icon, and then select **Start trial**.



16. When prompted, select **Start trial**.

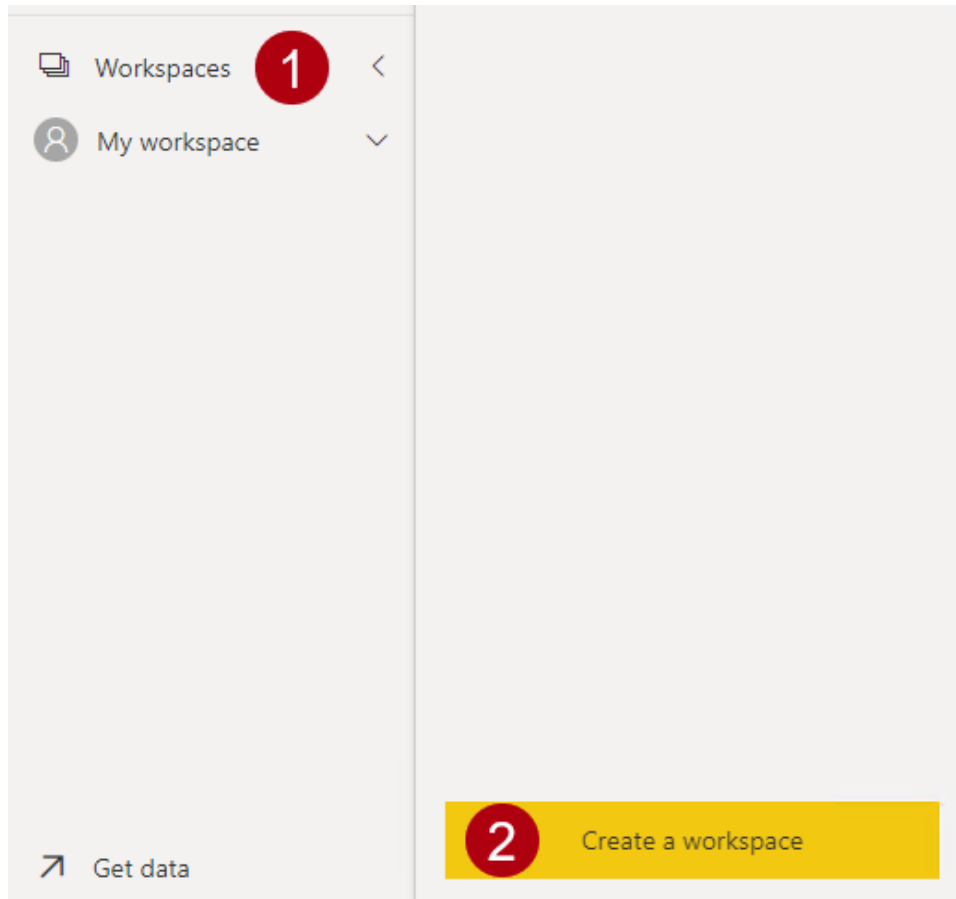
17. Do any remaining tasks to complete the trial setup.

*Tip: The Power BI web browser experience is known as the **Power BI service**.*

Create a workspace

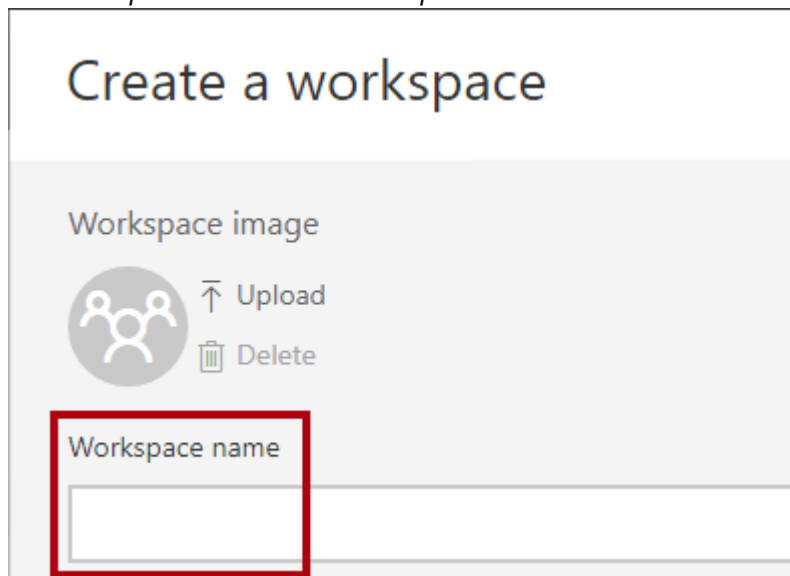
In this task, you will create a workspace.

18. In the Power BI service, to create a workspace, in the **Navigation** pane (located at the left), select **Workspaces**, and then select **Create workspace**.



19. In the **Create a workspace** pane (located at the right), in the **Workspace name** box, enter a name for the workspace.

The workspace name must be unique within the tenant.



20. Select **Save**.

Once created, the workspace is opened. In a later exercise, you will publish a dataset to this workspace.

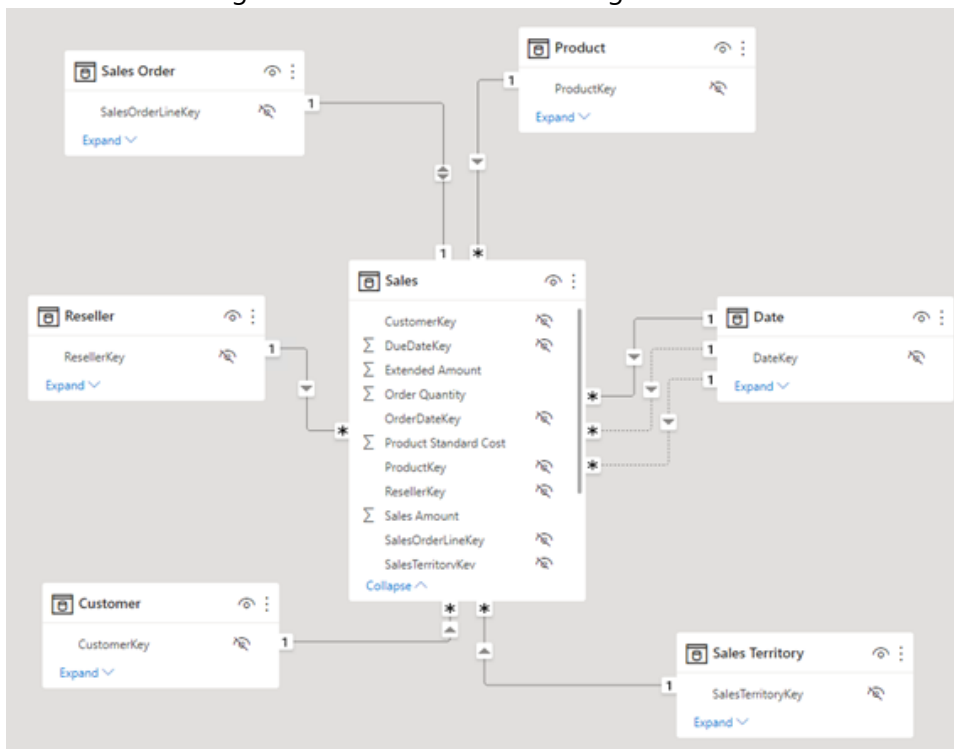
Review the data model

In this task, you will review the data model.

21. In Power BI Desktop, at the left, switch to **Model** view.

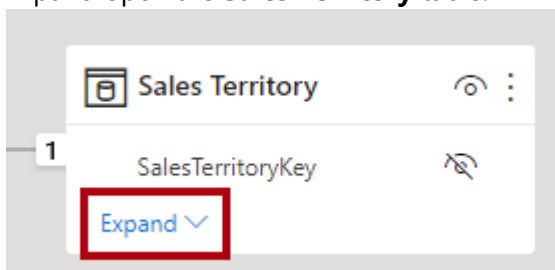


22. Use the model diagram to review the model design.



The model comprises six dimension tables and one fact table. The **Sales** fact table stores sales order details. It's a classic star schema design.

23. Expand open the **Sales Territory** table.



24. Notice that the table includes a **Region** column.

The **Region** column stores the Adventure Works sales regions. At this organization, salespeople are only allowed to see data related to their assigned sales region. In this lab, you will implement two different row-level security techniques to enforce data permissions.

Create static roles

In this exercise, you will create and validate static roles, and then see how you would map security principals to the dataset roles.

Create static roles

In this task, you will create two static roles.

25. Switch to **Report** view.



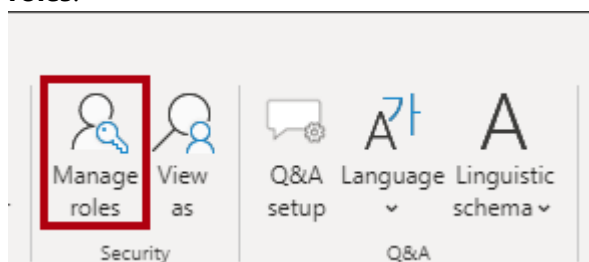
26. In the stacked column chart visual, in the legend, notice (for now) that it's possible to see many regions.

Sales Amount by Month and Region

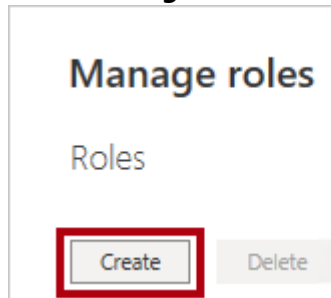
Region ● Australia ● Canada ● Central ● France ● Germany ● Northeast ● Northwest

For now, the chart looks overly busy. That's because all regions are visible. When the solution enforces row-level security, the report consumer will see only one region.

27. To add a security role, on the **Modeling** ribbon tab, from inside the **Security** group, select **Manage roles**.



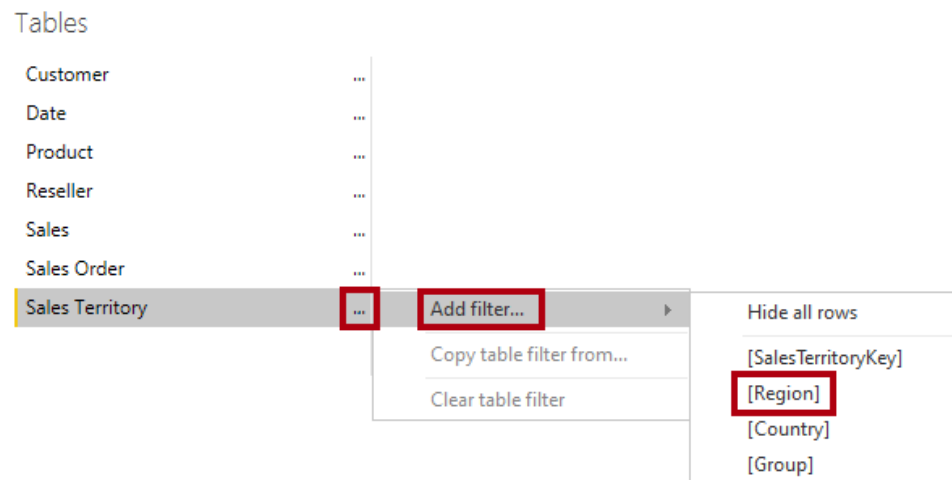
28. In the **Manage roles** window, select **Create**.



29. To name the role, replace the selected text with **Australia**, and then press **Enter**.



30. In the **Tables** list, for the **Sales Territory** table, select the ellipsis, and then select **Add filter > [Region]**.

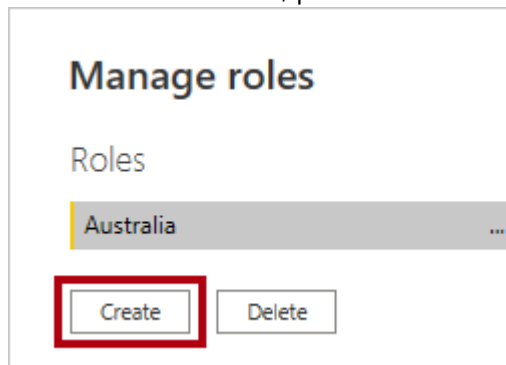


31. In the **Table filter DAX expression** box, replace **Value** with **Australia**.



*This expression filters the **Region** column by the value **Australia**.*

32. To create another role, press **Create**.



33. Repeat the steps in this task to create a role named **Canada** that filters the **Region** column by **Canada**.



In this lab, you'll create just the two roles. Consider, however, that in a real-world solution, a role must be created for each of the 11 Adventure Works regions.

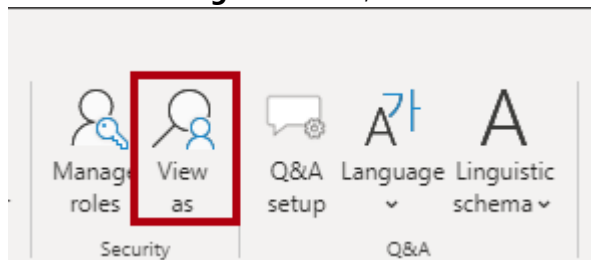
34. Select **Save**.



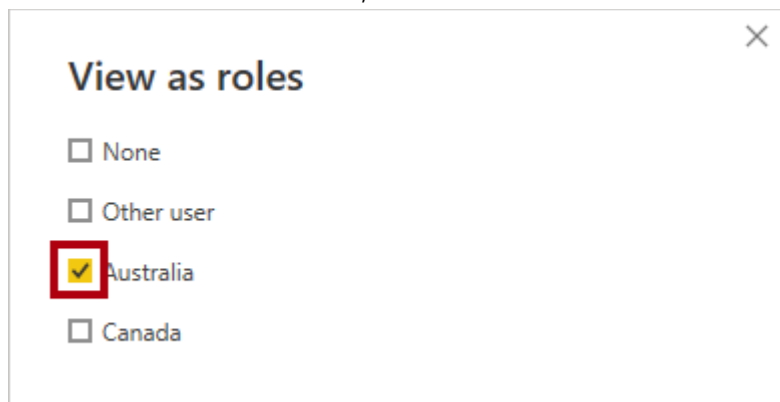
Validate the static roles

In this task, you will validate one of the static roles.

35. On the **Modeling** ribbon tab, from inside the **Security** group, select **View as**.



36. In the **View as roles** window, select the **Australia** role.



37. Select **OK**.

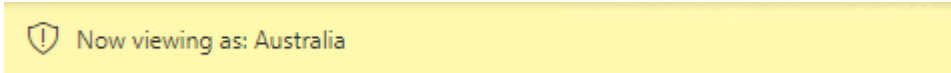


38. On the report page, notice that the stacked column chart visual shows only data for Australia.

Sales Amount by Month and Region

Region ● Australia

39. Across the top of the report, notice the yellow banner that confirms the enforced role.



40. To stop viewing by using the role, at the right of the yellow banner, select **Stop viewing**.



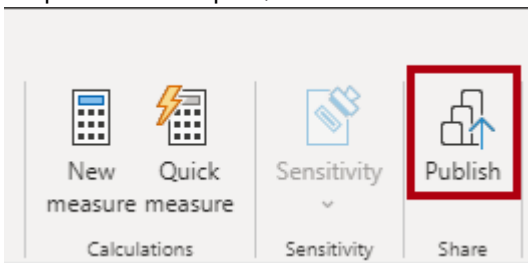
Publish the report

In this task, you will publish the report.

41. Save the Power BI Desktop file.



42. To publish the report, on the **Home** ribbon tab, select **Publish**.



43. In the **Publish to Power BI** window, select your workspace, and then select **Select**.

A screenshot of the 'Publish to Power BI' dialog box. The 'Select' button is highlighted with a red box. The 'Cancel' button is also visible.

44. When the publishing succeeds, select **Got it**.

A screenshot of a small dialog box with a single 'Got it' button, which is highlighted with a red box.

Configure row-level security (*optional*)



In this task, you will see how to configure row-level security in the Power BI service.

This task relies on the existence of a **Salespeople_Australia** security group in the tenant you are working in. This security group does NOT automatically exist in the tenant. If you have permissions on your tenant, you can follow the steps below. If you are using a tenant provided to you in training, you will not have the appropriate permissions to create security groups. Please read through the tasks, but note that you will not be able to complete them in the absence of the existence of the security group. **After reading through, proceed to the Clean Up task.**

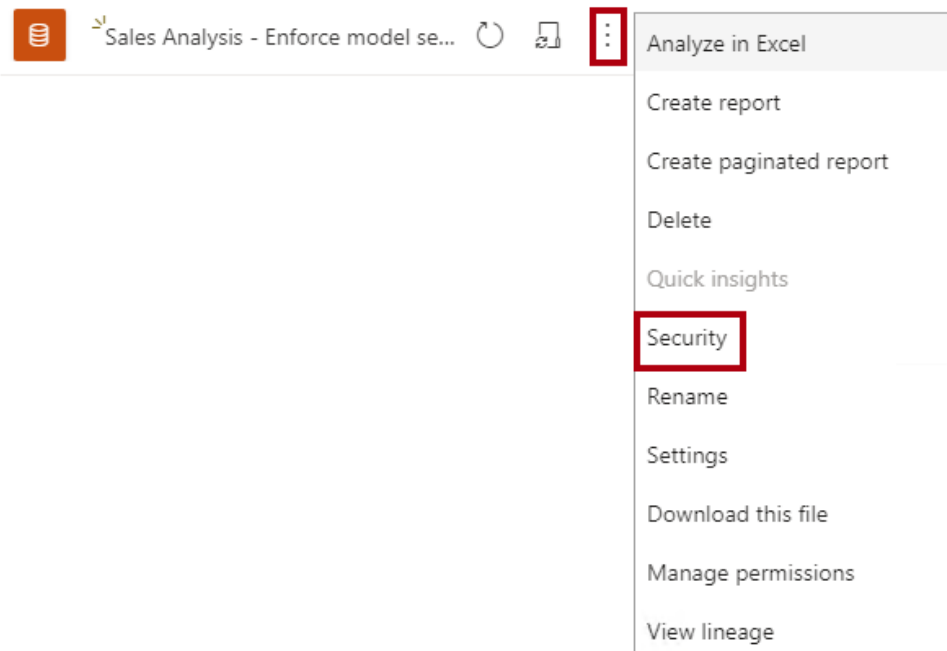
45. Switch to the Power BI service (web browser).

46. In the workspace landing page, notice the **Sales Analysis - Enforce model security** dataset.

All Content Datasets + dataflows

	Name	Type
	Sales Analysis - Enforce model security	Report
	Sales Analysis - Enforce model security	Dataset

47. Hover the cursor over the dataset, and when the ellipsis appears, select the ellipsis, and then select **Security**.



The screenshot shows a dataset named "Sales Analysis - Enforce model security" with a dataset icon. A red box highlights the ellipsis menu icon. The context menu is open, showing options: "Analyze in Excel", "Create report", "Create paginated report", "Delete", "Quick insights", "Security" (highlighted with a red box), "Rename", "Settings", "Download this file", "Manage permissions", and "View lineage".

The **Security** option supports mapping Microsoft Azure Active Directory (Azure AD) security principals, which includes security groups and users.

48. At the left, notice the list of roles, and that **Australia** is selected.



The screenshot shows the "Row-Level Security" configuration page. On the left, there is a list of roles: "Australia (0)" (selected) and "Canada (0)".

49. In the **Members** box, commence entering **Salespeople_Australia**.

Steps 5 through 8 are for demonstration purposes only, as they rely on the creation or existence of a *Salespeople_Australia* security group. If you have permissions and the knowledge to create security groups, please feel free to proceed. Otherwise, continue to the Clean Up task.

Members (0)

People or groups who belong to this role



Salespeople_

- Salespeople_Australia
- Salespeople_Canada

50. Select **Add**.



51. To complete the role mapping, select **Save**.



Now all members of the **Salespeople_Australia** security group are mapped to the **Australia** role, which restricts data access to view only Australian sales.

In a real-world solution, each role should be mapped to a security group.

This design approach is simple and effective when security groups exist for each region. However, there are disadvantages: it requires more effort to create and set up. It also requires updating and republishing the dataset when new regions are onboarded.

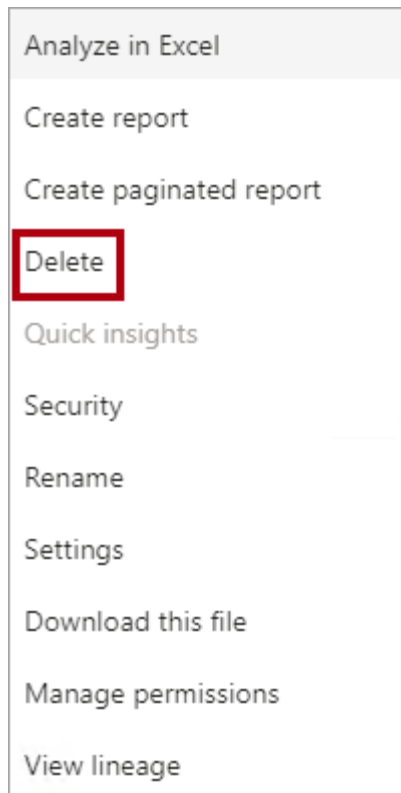
In the next exercise, you will create a dynamic role that is data-driven. This design approach can help address these disadvantages.

52. To return to the workspace landing page, in the **Navigation** pane, select the workspace.

Clean up the solution

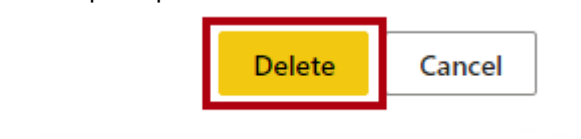
In this task, you will clean up the solution by removing the dataset and the model roles.

53. To remove the dataset, hover the cursor over the dataset, and when the ellipsis appears, select the ellipsis, and then select **Delete**.



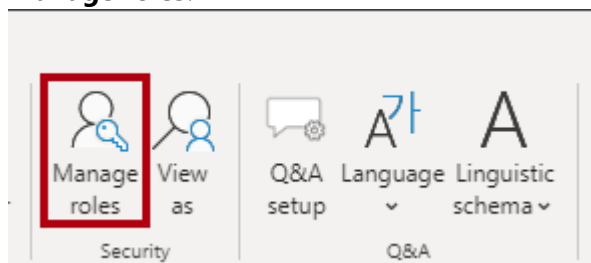
You will republish a revised dataset in the next exercise.

54. When prompted to confirm the deletion, select **Delete**.

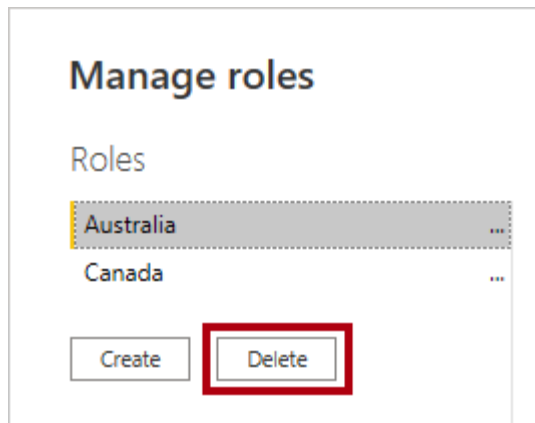


55. Switch to Power BI Desktop.

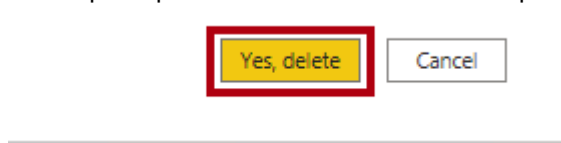
56. To remove the security roles, on the **Modeling** ribbon tab, from inside the **Security** group, select **Manage roles**.



57. In the **Manage roles** window, to remove the first role, select **Delete**.



58. When prompted to confirm the deletion, press **Yes, delete**.



59. Also remove the second role.

60. Select **Save**.



Create a dynamic role

In this exercise, you will add a table to the model, create and validate a dynamic role, and then map a security principal to the dataset role.

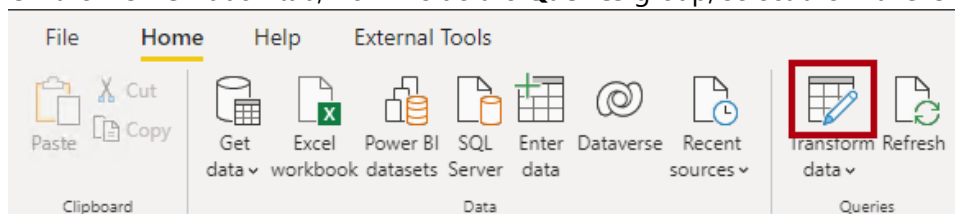
Add the Salesperson table

In this task, you will add the **Salesperson** table to the model.

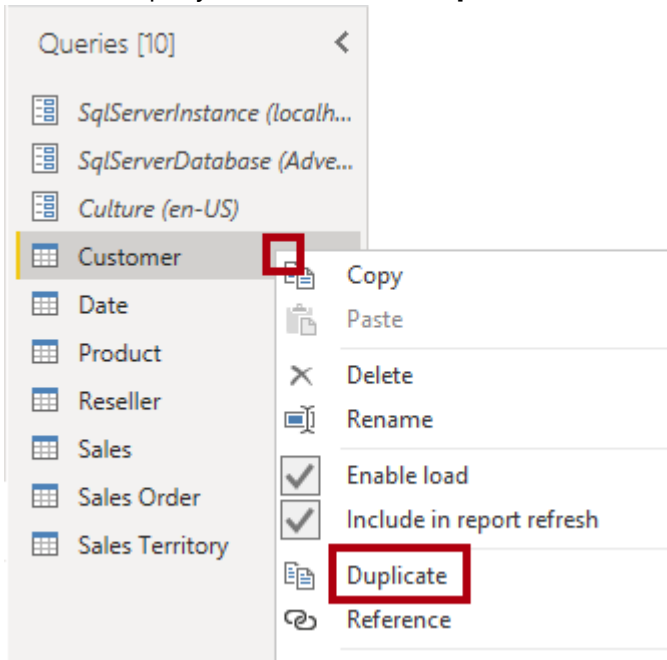
61. Switch to **Model** view.



62. On the **Home** ribbon tab, from inside the **Queries** group, select the **Transform data** icon.

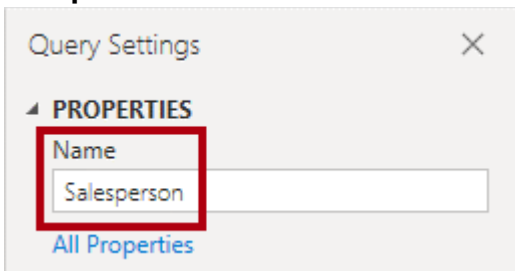


63. In the **Power Query Editor** window, in the **Queries** pane (located at the left), right-click the **Customer** query, and then select **Duplicate**.

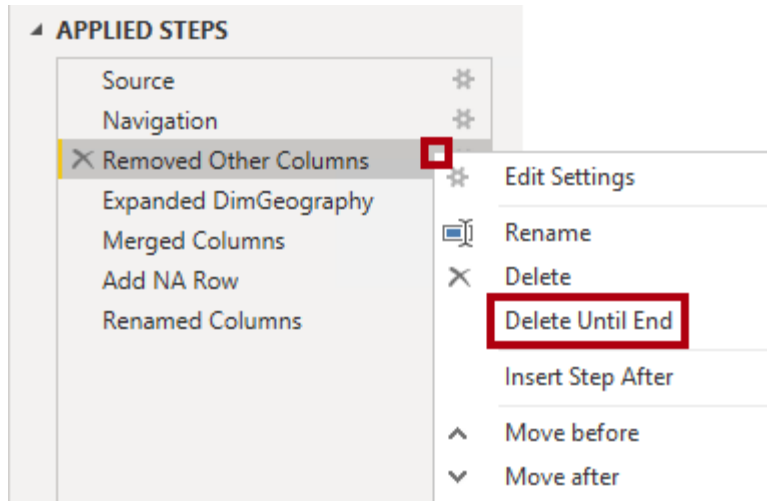


*Because the **Customer** query already includes steps to connect the data warehouse, duplicating it is an efficient way to commence the development of a new query.*

64. In the **Query Settings** pane (located at the right), in the **Name** box, replace the text with **Salesperson**.



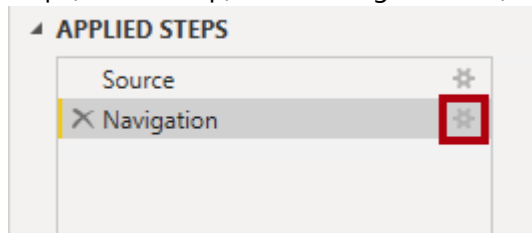
65. In the **Applied Steps** list, right-click the **Removed Other Columns** step (third step), and then select **Delete Until End**.



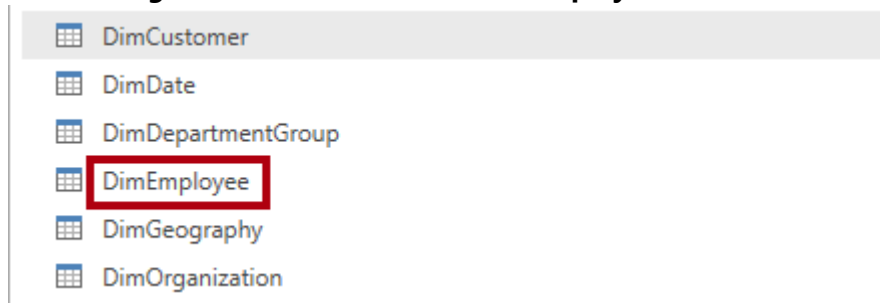
66. When prompted to confirm deletion of the step, select **Delete**.



67. To source data from a different data warehouse table, in the **Applied Steps** list, in the **Navigation** step (second step), select the gear icon (located at the right).



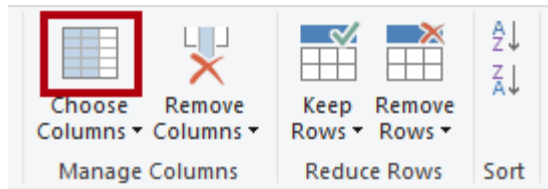
68. In the **Navigation** window, select the **DimEmployee** table.



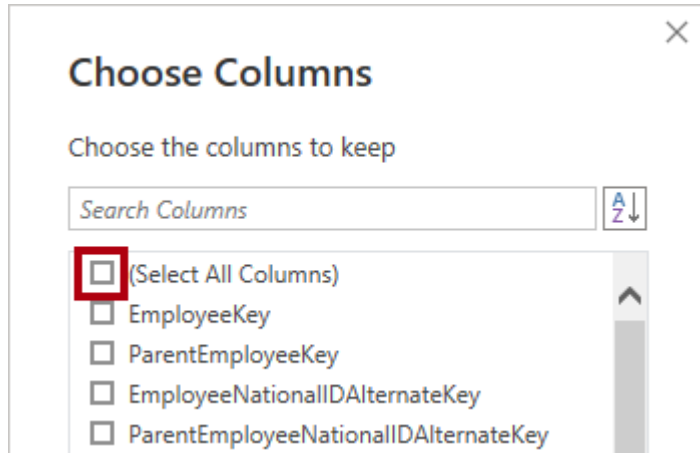
69. Select **OK**.



70. To remove unnecessary columns, on the **Home** ribbon tab, from inside the **Manage Columns** group, select the **Choose Columns** icon.



71. In the **Choose Columns** window, uncheck the **(Select All Columns)** item.



72. Check the following three columns:

- EmployeeKey
- SalesTerritoryKey
- EmailAddress

73. Select **OK**.



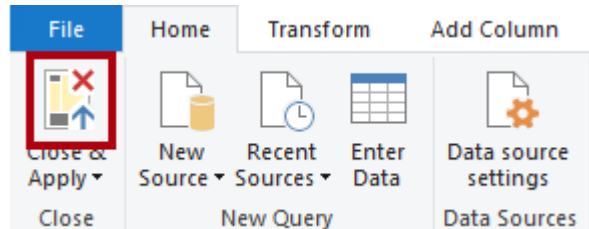
74. To rename the **EmailAddress** column, double-click the **EmailAddress** column header.

75. Replace the text with **UPN**, and then press **Enter**.

UPN is an acronym for User Principal Name. The values in this column match the Azure AD account names.

	123 EmployeeKey	123 SalesTerritoryKey	A ^B UPN
1	1	11	guy1@adventure-works.com
2	2	11	kevin0@adventure-works.com
3	3	11	roberto0@adventure-works.com

76. To load the table to the model, on the **Home** ribbon tab, select the **Close & Apply** icon.



77. When the table has added to the model, notice that a relationship to the **Sales Territory** table was automatically created.

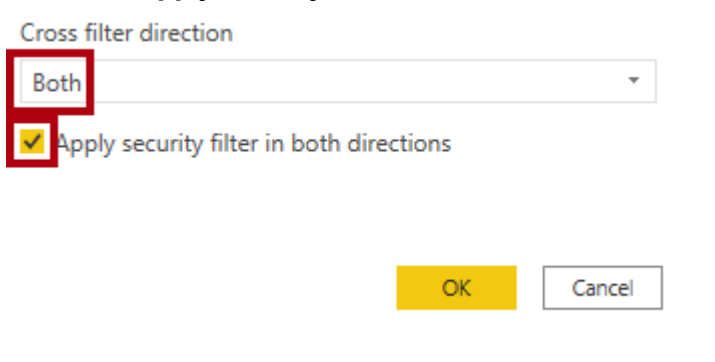
Configure the relationship

In this task, you will configure properties of the new relationship.

78. Right-click the relationship between the **Salesperson** and **Sales Territory** tables, and then select **Properties**.



79. In the **Edit relationship** window, in the **Cross filter direction** dropdown list, select **Both**.
80. Check the **Apply security filter in both directions** checkbox.

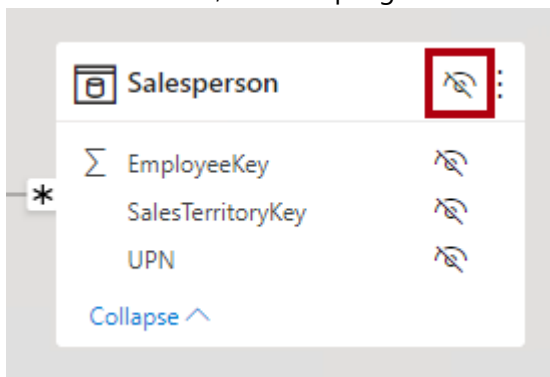


*Because there's a one-to-many relationship from the **Sales Territory** table to the **Salesperson** table, filters propagate only from the **Sales Territory** table to the **Salesperson** table. To force propagation in the other direction, the cross filter direction must be set to both.*

81. Select **OK**.



82. To hide the table, at the top-right of the **Salesperson** table, select the eye icon.



*The purpose of the **Salesperson** table is to enforce data permissions. When hidden, report authors and the Q&A experience won't see the table or its fields.*

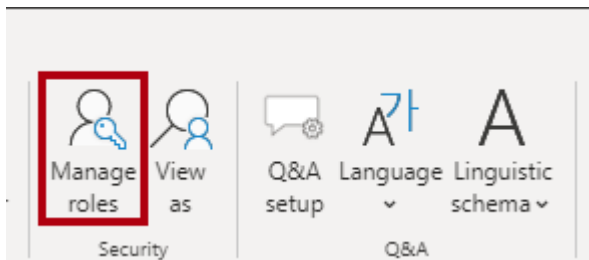
Create a dynamic role

In this task, you will create a dynamic role, which enforces permissions based on data in the model.

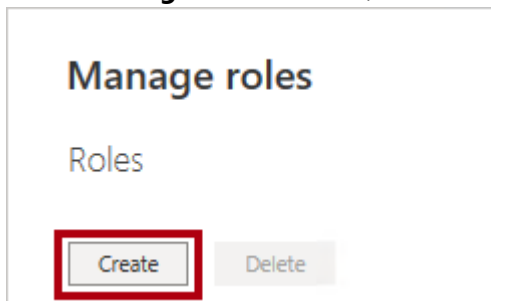
83. Switch to **Report** view.



84. To add a security role, on the **Modeling** ribbon tab, from inside the **Security** group, select **Manage roles**.



85. In the **Manage roles** window, select **Create**.

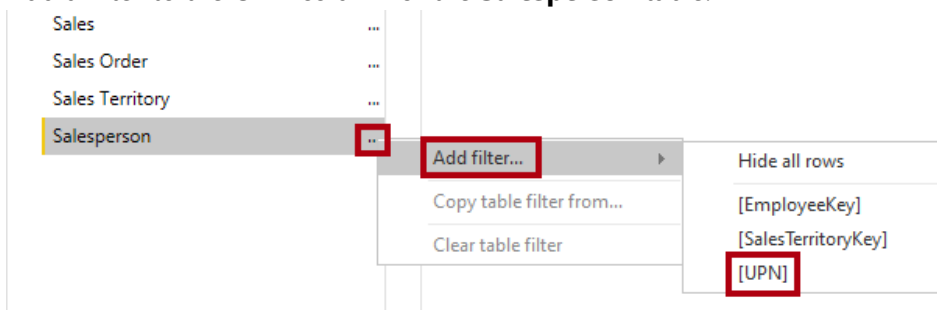


86. To name the role, replace the selected text with **Salespeople**.



This time, only one role needs to be created.

87. Add a filter to the **UPN** column of the **Salesperson** table.



88. In the **Table filter DAX expression** box, replace "**Value**" with **USERPRINCIPALNAME()**.

Table filter DAX expression

[UPN] = USERPRINCIPALNAME()

*This expression filters the **UPN** column by the **USERPRINCIPALNAME** function, which returns the user principal name (UPN) of the authenticated user.*

*When the UPN filters the **Salesperson** table, it filters the **Sales Territory** table, which in turn filters the **Sales** table. This way, the authenticated user will only see sales data for their assigned region.*

89. Select **Save**.

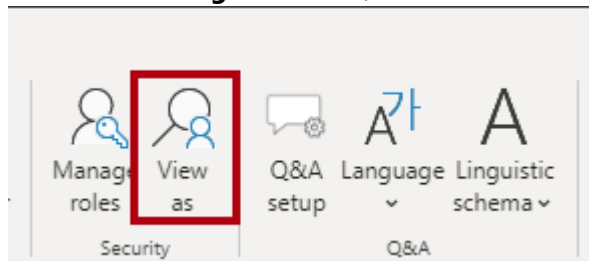
Save

Cancel

Validate the dynamic role

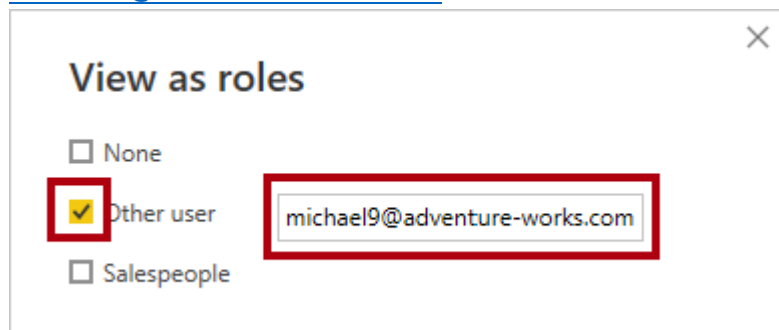
In this task, you will validate the dynamic role.

90. On the **Modeling** ribbon tab, from inside the **Security** group, select **View as**.



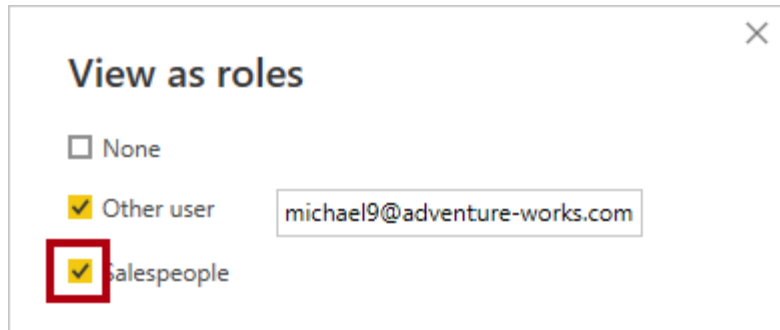
91. In the **View as roles** window, check **Other user**, and then in the corresponding box, enter:

michael9@adventure-works.com



*For testing purposes, **Other user** is the value that will be returned by the **USERPRINCIPALNAME** function. Note that this salesperson is assigned to the **Northeast** region.*

92. Check the **Salespeople** role.



93. Select **OK**.

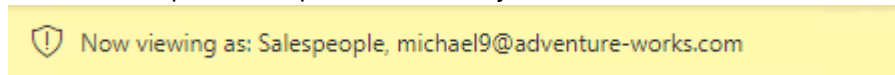


94. On the report page, notice that the stacked column chart visual shows only data for Northeast.

Sales Amount by Month and Region

Region ● Northeast

95. Across the top of the report, notice the yellow banner that confirms the enforced role.



96. To stop viewing by using the role, at the right of the yellow banner, select **Stop viewing**.



Finalize the design

In this task, you will finalize the design by publishing the report and mapping a security group to the role.

The steps in this task are deliberately brief. For full step details, refer to the task steps of the previous exercise.

97. Save the Power BI Desktop file.



98. Publish the report to the workspace you created at the beginning of the lab.

99. Close Power BI Desktop.

100. Switch to the Power BI service (web browser).

101. Go to the security settings for the **Sales Analysis - Enforce model security** dataset.

102. Map the **Salespeople** security group the **Salespeople** role.

Members (0)

People or groups who belong to this role

s

Salespeople

×

Enter email addresses

Now all members of the **Salespeople** security group are mapped to the **Salespeople** role. Providing the authenticated user is represented by a row in the **Salesperson** table, the assigned sales territory will be used to filter the sales table.

This design approach is simple and effective when the data model stores the user principal name values. When salespeople are added or removed, or are assigned to different sales territories, this design approach will simply work.

End the lab

Please be sure to end the lab(s) using the menu in the top right corner.

