



NAME: STEPHEN KYALO -ADC-DP01-25005

PROGRAM: DATA PROTECTION SPECIALIST

CLOUD SLICE TOPIC: MANAGE COMPLIANCE ROLES & MANAGE SENSITIVE INFORMATION
TYPES COMPLETION REQUIREMENTS

EXECUTIVE SUMMARY

The lab setup and environment preparation in Microsoft Purview involve configuring essential compliance and security settings. The process begins with resetting the passwords for three key users: Joni Sherman, Lynne Robbins, and Morgan Bowen. This step is crucial for establishing secure user access.

Next, auditing is enabled through the Purview portal or PowerShell to monitor user activity. The "Search by Name" feature is activated in Microsoft Teams to facilitate user identification, which is essential for configuring information barriers. These barriers are also enabled in SharePoint Online and OneDrive using PowerShell to ensure secure file collaboration.

Joni Sherman is assigned the Compliance Administrator role, which grants her the ability to manage compliance features across Microsoft 365. Additionally, the lab covers the management of Sensitive Information Types (SITs), including built-in, named entity, custom, and exact data match types, to aid in detecting and classifying sensitive data within the organisation.

EXECUTIVE SUMMARY.....2

GLOSSARY.....2

1. LAB SETUP AND ENVIRONMENT PREPARATION..... 2

2. MANAGE COMPLIANCE ROLES..... 5

3. MANAGE SENSITIVE INFORMATION TYPES..... 7

1. LAB SETUP AND ENVIRONMENT PREPARATION

This stage evolves around configuring and preparing the cloud environment for administrative tasks. The process begins with resetting the passwords of three users: Joni Sherman, Lynne Robbins, and Morgan Bowen. Each user account is assigned a single custom password as shown below.

The screenshot displays the Microsoft 365 admin center interface. The main content area shows a list of users with checkboxes for selection. The users listed are Joni Sherman, Lee Gu, Lidia Holloway, Lynne Robbins, Megan Bowen, and Miriam Graham. The right sidebar contains instructions for resetting passwords and enabling audit in the Purview portal. The instructions include steps for selecting the 'Reset password' button and navigating to the Purview portal to enable audit logging.

Display name	Username	Licenses
<input checked="" type="checkbox"/> Joni Sherman	JoniS@WWLx097506.OnMicrosoft.com	Microsoft Teams Enterprise, Microsoft Teams
<input type="checkbox"/> Lee Gu	LeeG@WWLx097506.OnMicrosoft.com	Microsoft Teams Enterprise, Microsoft Teams
<input type="checkbox"/> Lidia Holloway	LidiaH@WWLx097506.OnMicrosoft.com	Microsoft Teams Enterprise, Microsoft Teams
<input checked="" type="checkbox"/> Lynne Robbins	LynneR@WWLx097506.OnMicrosoft.com	Microsoft Teams Enterprise, Microsoft Teams
<input checked="" type="checkbox"/> Megan Bowen	MeganB@WWLx097506.OnMicrosoft.com	Microsoft Teams Enterprise, Microsoft Teams
<input type="checkbox"/> Miriam Graham	MiriamG@WWLx097506.OnMicrosoft.com	Microsoft Teams Enterprise, Microsoft Teams

Task - Enable Audit in the Microsoft Purview portal

In this task, you'll enable Audit in the Microsoft Purview portal to monitor portal activities.

1. You should still be logged into Client 1 VM (SC-400-CL1) as the SC-400-CL1admin account and logged into Microsoft 365 with the MOD Administrator account.
2. In Microsoft Edge, navigate to the Microsoft Purview portal, <https://purview.microsoft.com>, and log in.

The next step is to enable Auditing through the Audit feature in the Purview Portal. This allows monitoring of the Purview portal activities.

The screenshot displays the Microsoft Purview Audit page. The main content area shows the 'Start recording user and admin activity' button. The right sidebar contains instructions for enabling audit logging. The instructions include steps for selecting 'Solutions' from the left sidebar, selecting 'Audit', and clicking the 'Start recording user and admin activity' button.

Search

Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page.

Start recording user and admin activity

Searches completed | Active searches | Active unfiltered searches

Date and time range (UTC) *

Start

May 17 2025

00:00

Task - Enable Audit in the Microsoft Purview portal

In this task, you'll enable Audit in the Microsoft Purview portal to monitor portal activities.

4. Select **Solutions** from the left sidebar, then select **Audit**.
5. On the **Search** page, select the **Start recording user and admin activity** bar to enable audit logging.
6. Once you select this option, the blue bar should

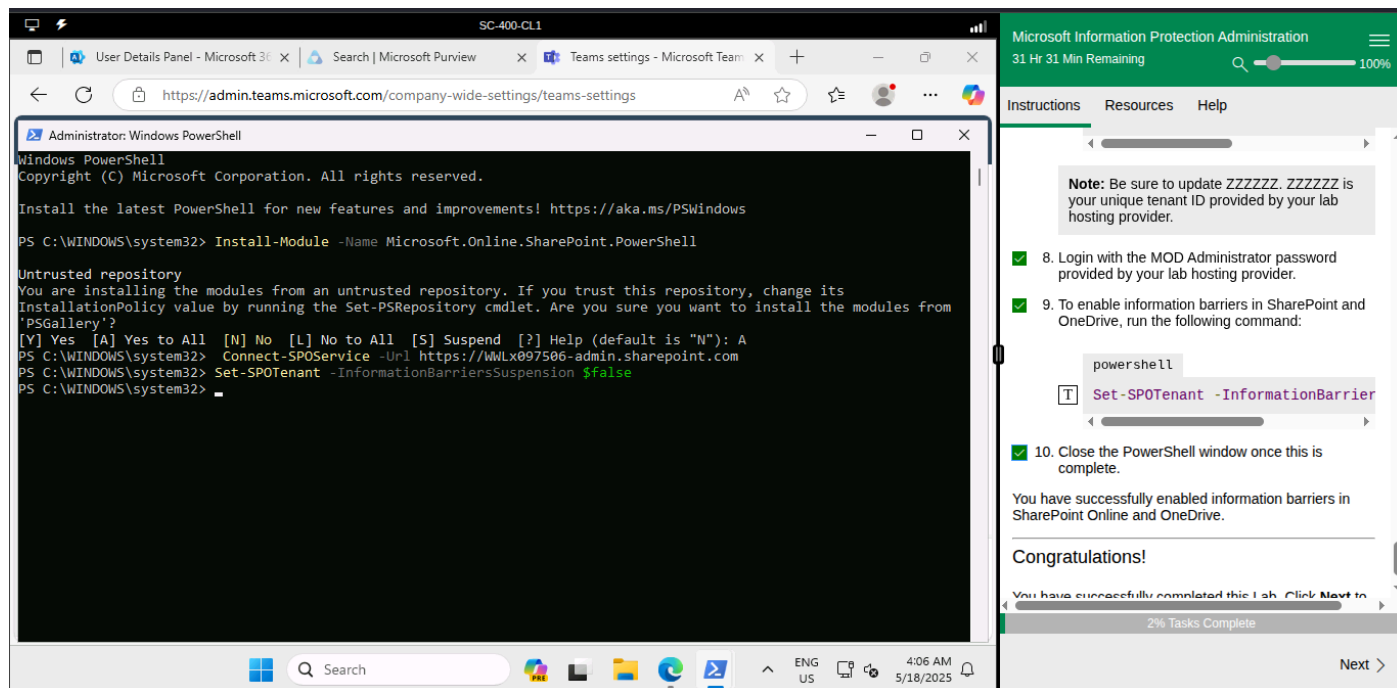
Auditing can also be enabled through PowerShell with elevated privileges if enabling it through the portal fails.

The screenshot shows a PowerShell terminal window on the left and the Microsoft Information Protection Administration portal on the right. The terminal window displays the command `Install-Module -Name ExchangeOnlineManagement` and the output, which includes instructions for installing the module from an untrusted repository and connecting to Exchange Online. The portal window shows the 'Instructions' tab with a list of steps for enabling audit logging, including running `Get-AdminAuditLogConfig` and `Set-AdminAuditLogConfig` with the `UnifiedAuditLogIngestionEnabled` parameter set to `$true`.

Next is enabling the **Search by name** feature in Microsoft Teams to enable easy user location. Search by name is enabled through the Microsoft Teams Admin center. This is needed for configuring information barriers later on in the lab exercise.

The screenshot shows the Microsoft Teams Admin Center on the left and the Microsoft Information Protection Administration portal on the right. The Teams Admin Center displays the 'Search by name' section, which includes a toggle for 'Scope directory search using an Exchange address book policy' set to 'On'. The portal window shows the 'Instructions' tab with a list of steps for enabling search by name, including selecting 'Teams settings' and toggling the 'Scope directory search using an Exchange address book policy' to 'On'.

After enabling the **Search by name** feature, we need to enable Information barriers in SharePoint Online and OneDrive through PowerShell. This ensures the security of collaboration files stored in both OneDrive and SharePoint.



2. MANAGE COMPLIANCE ROLES

The user Joni Sherman is assigned Compliance Administrator roles and given access to admin centres. The Compliance Administrator role enables Joni to **manage compliance-related features and data** across Microsoft 365. This role is especially useful for those responsible for overseeing regulatory compliance, risk management, and data protection. This is demonstrated below.

SC-400-CL1

User Details Panel - Microsoft 365 | Search | Microsoft Purview | Teams settings - Microsoft Teams | +

https://admin.microsoft.com/Adminportal/Home#/users/managerbacroles/userData...

Contoso Electronics | Microsoft 365 admin center

Manage admin roles

Joni Sherman selected

Admin roles updated

Admin roles give users permission to view data and complete tasks in admin centers. Give users only the access they need by assigning the least-permissive role.
[Learn more about admin roles](#)

User (no admin center access)

Admin center access

Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned

Save changes

Search

ENG US | 4:18 AM 5/18/2025

Microsoft Information Protection Administration

31 Hr 18 Min Remaining

Instructions Resources Help

then select **Joni Sherman**.

5. The properties for Joni's account is displayed in a right, flyout panel. Select **Manage roles** on the flyout panel.

6. On the **Manage admin roles** panel, select the option for **Admin center access**, then scroll down to expand **Show all by category**.

7. Under the **Security & Compliance** category, select the checkbox for **Compliance Administrator**, then select **Save changes** at the bottom of the flyout panel.

8. You should receive a message stating **Admin roles updated**.

9. On the **Manage admin roles** page, select the **X** on the top right corner of the flyout panel to close the panel.

10. Sign out of the MOD Administrator account by selecting the **MA** icon in the top right, then select **Sign out**.

2% Tasks Complete

Previous Next

SC-400-CL1

User Details Panel - Microsoft 365 | Search | Microsoft Purview | Teams settings - Microsoft Teams | +

https://admin.microsoft.com/Adminportal/Home#/users/managerbacroles/userData...

Contoso Electronics | Microsoft 365 admin center

Manage admin roles

Joni Sherman selected

Security & Compliance

Attack Payload Author ⓘ

Attack Simulation Administrator ⓘ

Azure Information Protection Administrator ⓘ

Compliance Administrator ⓘ

Save changes

Search

ENG US | 4:11 AM 5/18/2025

Microsoft Information Protection Administration

31 Hr 26 Min Remaining

Instructions Resources Help

admin@wmlx897586.onmicrosoft.com
Admin's password should be provided by your lab hosting provider.

3. On the left sidebar, expand **Users** then select **Active users**.

4. On the **Active users** page, search for **Joni**, then select **Joni Sherman**.

5. The properties for Joni's account is displayed in a right, flyout panel. Select **Manage roles** on the flyout panel.

6. On the **Manage admin roles** panel, select the option for **Admin center access**, then scroll down to expand **Show all by category**.

7. Under the **Security & Compliance** category, select the checkbox for **Compliance Administrator**, then select **Save changes** at the bottom of the flyout panel.

8. You should receive a message stating **Admin roles updated**.

9. On the **Manage admin roles** page, select the **X** on the top right corner of the flyout panel to close the panel.

2% Tasks Complete

Previous Next

3. MANAGE SENSITIVE INFORMATION TYPES

Sensitive Information Types (SITs) are pattern-based data classifiers. They detect sensitive information like credit card numbers, invoice numbers or social security numbers. SITs are categorised into:

- Built-in SITs- these come with the Purview Portal by default and can be edited to create custom SITs
- Named entity SITs- these also come with Purview by default and detect names of people, physical addresses, and medical terms and conditions.
- Custom SITs- created by administrators to fit the needs of their organisations. They can be created by fully defining new SITs or modifying built-in SITs.
- Exact Data Match (EDM)- detects sensitive data by matching exact values from a defined secured database.

Below is a demonstration of creating custom SITs in the Microsoft Purview Portal.

Microsoft Information Protection Administration
30 Hr 54 Min Remaining

Instructions Resources Help

14. Select **Done** at the bottom of the flyout panel.

15. Back on the **New pattern** flyout panel, under **Character proximity**, decrease the **Detect primary AND supporting elements** value to **100** characters.

16. Select the **Create** button at the bottom of the flyout panel.

17. Back on the **Define patterns for this sensitive info type** page select **Next**.

18. On the **Choose the recommended confidence level to show in compliance policies** page use the default value and select **Next**.

19. On the **Review settings and finish** page review the settings and select **Create**. When successfully created select **Done**.

20. Sign out of Joni's account by selecting the profile picture of Joni Sherman in the top right. Select **Sign out**, then close the browser window.

21. Close the browser window then open a new browser window.

You have successfully created a new sensitive

3% Tasks Complete

< Previous Next >

Microsoft Information Protection Administration
30 Hr 52 Min Remaining

Instructions Resources Help

14. Select **Done** at the bottom of the flyout panel.

15. Back on the **New pattern** flyout panel, under **Character proximity**, decrease the **Detect primary AND supporting elements** value to **100** characters.

16. Select the **Create** button at the bottom of the flyout panel.

17. Back on the **Define patterns for this sensitive info type** page select **Next**.

18. On the **Choose the recommended confidence level to show in compliance policies** page use the default value and select **Next**.

19. On the **Review settings and finish** page review the settings and select **Create**. When successfully created select **Done**.

20. Sign out of Joni's account by selecting the profile picture of Joni Sherman in the top right. Select **Sign out**, then close the browser window.

21. Close the browser window then open a new browser window.

You have successfully created a new sensitive

3% Tasks Complete

< Previous Next >

Creation of EDM classifiers demonstration.

Microsoft Purview

EDM classifiers > Create EDM classifier

✓ Name your classifier

✓ Define the schema

✓ Specify detection rules

● Review and finish

EDM classifier description

Employee Database schema

[Edit EDM classifier description](#)

Sensitive info types for primary elements

EmployeeID - Contoso Employee IDs

[Edit sensitive info types for the most critical sensitive data](#)

Schema file column settings

Data in all columns is case insensitive

Ignored punctuation and delimiters for all fields - Hyphen ('-'), Period ('.'), Space (' '), Open parenthesis ('('), Close parenthesis (')')

[Edit schema file column settings](#)

Detection rules

EmployeeID - 2 confidence levels (High, Medium)

[Edit detection rules](#)

Back

Submit

Cancel

Microsoft Information Protection Administration

30 Hr 6 Min Remaining

Instructions Resources Help

Identify this field as a Primary element.

EmployeeID

Contoso Employee IDs

33. Select Next.

34. On the **Configure settings for data in selected columns**, ensure the toggle is set to **Yes for Use the same settings for all columns**.

35. Select the checkbox for **Ignore delimiters and punctuation for data in all columns**.

36. Select the dropdown for **Choose delimiters and punctuation to ignore** dropdown and select **Hyphen, Period, Space, Open parenthesis and Close parenthesis**, then select **Next**.

37. On the **Configure detection rules for primary elements**, leave the default configuration, then select **Next**.

38. On the **Review settings and finish** page, select **Submit**.

39. On the **You successfully created an EDM classifier** page, be sure to copy and paste the **Schema name** to use in the next task.

7% Tasks Complete

Previous

Next

Microsoft Purview

EDM classifiers

Home

Solutions

Learn

Settings

Information Protection

Information Protection

Overview

Reports

Recommendations

Sensitivity labels

Policies

Classifiers

Trainable classifiers

Sensitive info types

EDM classifiers

On-demand classification

New EDM experience

Why are there two experiences?

Exact data match (EDM) classifiers use exact values from your org's data to detect matches instead of generic patterns. They can then be included in several compliance solutions to classify and protect sensitive data. [Learn more about EDM](#)

Create EDM classifier

1 item

Search

Name ↑	Created by	Status
<input type="checkbox"/> employeedb	Contoso	Source file not uploaded yet How

Microsoft Information Protection Administration

30 Hr 5 Min Remaining

Instructions Resources Help

elements, leave the default configuration, then select **Next**.

38. On the **Review settings and finish** page, select **Submit**.

39. On the **You successfully created an EDM classifier** page, be sure to copy and paste the **Schema name** to use in the next task.

Schema name

employeedbSchema

Copy

40. Once you've captured the schema name, select **Done**.

41. Leave the browser open with the Microsoft Purview portal.

You have successfully created a new EDM-based classification sensitive information type for identifying employee data from a database file source.

Task 3 – Create EDM-based classification data source

7% Tasks Complete

Previous

Next