Microsoft Endpoint DLP Interactive Guide

Overview

Unified DLP is an integral component of our Microsoft 365 Information Protection suite that gives you broad visibility and control over the lifecycle of your sensitive information as it's used and shared by your users across your organization. Our data loss prevention solution works across various Cloud services. After completing this interactive guide, you will understand how to configure our endpoint data-loss prevention capabilities as an administrator and subsequently validate them as an end-user.

Exercise 1: Overview of the Microsoft 365 Compliance Center

1. ☐ Click to place focus in the address bar of Microsoft Edge and then type https://compliance.microsoft.com/ and hit enter to navigate to the Microsoft 365 compliance center.
2. ☐ Sign in with the following credentials (select the checkbox to stay signed in.)
    - admin@contoso.com
    - Password: Password
    - On stay signed in dialogue box, click **Yes**.

    (Note: You may get a **Save Password** dialogue box at the top right. Just click on **Never**.)

3. ☐ You have entered the **Microsoft 365 compliance center**. Your home for managing your compliance needs. Click below the **scroll bar** on the lower right. Note the overall compliance score and solutions catalog sections.
4. ☐ Click below the **scroll bar** on the lower right again – Note High-Risk Apps and Retention label sections.
5. ☐ Click below the **scroll bar** on the lower right again – Note this will show any active alerts.

Congratulations, you have seen a quick overview of the Microsoft 365 compliance center.

Exercise 2: Review of Endpoint DLP Settings

Before you start configuring a specific DLP policy, you should set up your global DLP settings applied to all DLP policies for devices. You must configure these if you intend to create policies that enforce cloud egress restrictions, unallowed apps restrictions, or need to exclude noisy file paths from monitoring. This exercise will walk you through how to check for these global settings.

1. ☐ Click on the **Data loss prevention** section on the lower part of the left navigation menu. This will open the **Data loss prevention** page (Note: These are the policies used to manage this organization's data loss prevention.)
2. ☐ Click on **Endpoint DLP settings**
3. ☐ With **Data loss prevention** still at the top, click on the **File path exclusions** down arrow.

4. ☐ Click on **+Add file path exclusion.** Here you can adjust the paths upon which sensitive data is automatically scanned. For example, you may want to exclude an application data-path that includes various temporary files and content that is not generally subject to the policies you are concerned with.
5. ☐ Click on the **Cancel** button.
6. ☐ Click on the **up arrow** to the right of **File path Exclusion** to close this section.
7. ☐ Click on **the Unallowed apps** down arrow to the right.
8. ☐ Click on **+ Add unallowed apps.** Here you can adjust which applications users will be allowed to access sensitive data as deemed by the organization's DLP policy controls.
9. ☐ Click on the **Cancel** button.
10. ☐ Click on the **up arrow** to the right of **Unallowed Apps** to close this section.
11. ☐ Click on the **down arrow** to the right of **Browser and domain restrictions to sensitive data**.
12. ☐ Click below the **scroll bar** on the lower right to move down.
13. ☐ Under Unallowed Browsers Click on **+ Add Unallowed browsers**. Here you can limit or allow what browsers can access company resources as defined through your custom DLP policy controls that you will set up later in this Interactive Guide. (Note: We have already added Firefox, Google Chrome, and SeaMonkey that will be restricted in the organization's DLP policies.)
14. ☐ Click on the **Cancel** button.
15. ☐ Under Service domains, click on **+ Add service domain**. Here you can limit or allow what service domains can access sensitive data as defined through your custom DLP policy controls that you will set up later in this Interactive Guide.
16. ☐ Click on the **Cancel** button.
17. ☐ Click on the **Scroll Bar** at the top right to scroll back up the page where it will say **Data loss prevention** at the top.

Congratulations, you have completed Exercise 2 - Review of Endpoint DLP Settings

Exercise 3: Creating and Reviewing DLP Policy for Endpoints

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are on Windows 10 devices. Once devices are onboarded into the Microsoft 365 compliance solutions, the information about what users are doing with sensitive items is made visible in the Activity Explorer, and you can enforce protective actions on those items via DLP policies.

Device management is the functionality that enables the collection of telemetry from devices and brings it into Microsoft 365 compliance solutions like Endpoint DLP and Insider Risk management. You'll need to onboard all devices you want to use as locations in DLP policies.

This exercise will take you through configuring your organization's DLP policies. We will walk through both the Template-Simple Path View (Note: This includes about 80% of what a typical administrator would do.) and an overview of the Custom section.

3.1 Configuration Using the Template

1. ☐ At the top of the **Data loss prevention** page, click on the **Policies tab.**
2. ☐ With the **Policies** tab selected, click on **+ Create policy**.
3. ☐ In the **Start with a template or create a custom policy section**, under Categories click on **Financial.**
4. ☐ In the **Templates** column, click on the **scroll bar** at the right to move down.
5. ☐ Then click on **PCI Data Security Standard (PCI DSS)** in the Templates column. (Note: this policy will protect credit card data and other types of financial PII data in my organization.)
6. ☐ Click on the **Next** button at the bottom.
7. ☐ In the **Name your DLP Policy** section, click in the **Name** entry box. Type in – **Contoso EP - PCI Data Security Policy** and hit **Enter**.
8. ☐ Click in the Description entry box and type in - **Policy to protect credit card and other types of financial PII data** and hit **Enter**.
9. ☐ Click on the **Next** button at the bottom.
10. ☐ In the **Choose locations to apply the policy** section**,** you will need to turn off all locations except for **Devices**. This is the policy you are creating. Click the **Status** button to the left to **Off** for each of these (Except for Devices):
    - Exchange email
    - SharePoint sites
    - OneDrive accounts
    - Teams chat and channel messages
    - Microsoft Cloud App Security
    - On-Premises Scanner
11. ☐ Leave the **Status** button for **Devices** to **On**. Click on the **Next** button at the bottom.
12. ☐ In the **Define Policy settings** section**,** click on the **Next** button.
13. ☐ In the **Info to protect** section – click on the **Edit** button under Credit Card Number.
14. ☐ In **Choose the types of content to protect** under Credit Card Number, click on the **Add** down arrow.
15. ☐ Click on **Sensitive info types.**
16. ☐ In the **Sensitive info types** dialogue box, click in the Search box and type in **debit**, and hit **Enter**.
17. ☐ Select the check box for **EU Debit Card Number.**
18. ☐ Click on **Add** at the bottom of the page.
19. ☐ You are back at the **Choose the types of content to protect** section. At the top right, click on **Any of these**. (Note: You could select **All of these,** which would only trigger an

action if all Sensitive Info conditions below occurred.) In this case, keep the drop-down box at **Any of these**.

20. ☐ Click in the far-right **Instance count** box for EU Debit Card and type in **9** and hit **Enter.**

    A few notes here: The higher the accuracy percentage, the more precision you wil have with fewer false positives. If you lower the accuracy, you might catch numbers that look like a credit card but are not a credit card number. Your organization gets to select the accuracy level to indicate how broad or how narrow they want the scope of the detection. The instance count is specific to the number of unique instances that data is detected.

21. ☐ Click on the **Add** down arrow on the left under EU Debit Card Number.
22. ☐ Click on **Sensitivity labels.** (Note: Microsoft is creating DLP policy rules to protect data that has been assigned sensitivity labels. Currently, we have been using Highly Confidential and Project Obsidian labels in this exercise. Project Obsidian is a new research and development initiative at our organization for which we need to create a new DLP policy.)
23. ☐ In the **Sensitivity labels** section, select the check box for **Highly Confidential.**
24. ☐ Select the check box for **Project Obsidian.**
25. ☐ Click on the **Add** button.
26. ☐ Click on the **Save** button (Note: This Policy will protect Credit Card Numbers, EU Debit Card Numbers, and Highly Confidential Information in any documents or credit cards a user may try to share.)
27. ☐ In the **Info to protect** section, click on **Next** button.
28. ☐ In the **Protection actions** section, click on **Customize the tip and email**.
29. ☐ The **Customize policy tips and email notifications** section allows you to customize any policy tips or notifications displayed to a user that tries to access, send or copy any highly confidential or credit/debit card information. In this case, we will just use the defaults. Click on the **Cancel** button.
30. ☐ Leave the check box checked by **Detect when a specific amount of sensitive info is being shared at one time**. Leave the **At least** box at 10. Click on **Customize alert configuration.** This section tells the service to send email alerts to designated people in the group as defined by the administrator.
31. ☐ Click on the **Send alert when the volume matched activities reaches a threshold** button.
32. ☐ Click on the **Instances more than or equal to matched activities** check box and click in the box at right and type in **5** and hit **Enter.** (Note: This is especially good for monitoring when a person in the organization has performed 5 or more instances of copying or sending highly confidential information outside the organization.)
33. ☐ Click on the **Volume more than or equal to MB** check box and click in the box at the right and type in **5** and hit **Enter.** This is good for tracking many highly confidential documents being printed or large amounts of data being accessed.
34. ☐ Click on the **Save** button. You will be back at the main **Protection actions** section.
35. ☐ Note the **Restrict access or encrypt the content in Microsoft 365 locations is greyed out**. If this DLP policy was on a Microsoft 365 service, you could restrict access by clicking

this checkbox. Click on the **Next** button. You are now in the **Customize access and override settings** section.

36. ☐ Click on the **Audit or restrict activities on the Windows devices check box**. Here is where you can either fully block, block with the ability to override, or audit any of these activities on Windows devices that have been onboarded. Audit is often used to test policies before they become "live" or to monitor activities without impacting users with popups. Block with override gives the users the ability to continue with the action that triggered the policy, for when a user has a legitimate business need to complete the action. Block will not allow the user to override the block action.
37. ☐ In the **Upload to cloud services or access by unallowed browsers,** click on the **down arrow** to the right and select **Block**. Users will not be able to upload any files with sensitive information to unallowed browsers you have already confirmed in the Browser and Domain restrictions to sensitive data global section in exercise 2.
38. ☐ Click on the **down arrow** to the right of **Copy to Clipboard** and select **Block with Override**. This will warn the user they are trying to copy sensitive information but allows them to override.
39. ☐ For the other activities:
    - ☐ Click on the right **down arrow** by **Copy to a USB removable media** – Click on **Block.** This will block this activity with a description of why.
    - ☐ Click on the right **down arrow** by **Copy to a network share** – Click on **Block with override.** This will block this activity initially but allow them to override.
    - ☐ Click on the right **down arrow** by **Access by unallowed apps** – Click on **Block.** This will block this activity with a description of why.
    - ☐ Click on the right **down arrow** by **Print** – Click on **Block with override.** This will block this activity initially but allow them to override.
40. ☐ Click on the **Next** button at the bottom.
41. ☐ In the **Test or turn on the policy** section, if you click on test it out first, you will be able to test the policy to ensure it works correctly prior to deploying. Leave **I'd like to test it out first** selected for now. Click on the **Next** button at the bottom.

    Review your policy on the **Review your policy and create it** page. Note this is for any Windows Devices that have been onboarded to this group.

42. ☐ Sometimes there will be a need to create a fully customized DLP policy instead of using a default template. In our next example, we will cover the options available to customize the policy. For simplicity, we will just step back in our UI and go to the customizations options screen. Click on **Back** and click on **Back** again to get back to the **Define Policy Settings** section.

3.2 Overview of Custom Configuration

1. ☐ In the **Define policy settings** section, click in the circle for **Create or customize advanced DLP rules**

2. ☐ Click on the **Next** button.
3. ☐ In the **Customize advanced DLP rules** section, we will only show one advanced rules area, so click on the **Pencil icon** under the **Edit** column for **High Volume of content detected PCI DSS**. (Note: This is a deeper break out of what was seen in the **Define policy settings** section in the existing DLP Template for Credit Card Number.)
4. ☐ In the **Edit rule** section, click on the **scroll bar** to the lower right to move down the page.
5. ☐ Under Exceptions, click on **+Add exception.**
6. ☐ Click on **Except if content contains** (Note: Here, you can add additional Conditions and Exceptions.)
7. ☐ Click on the **scroll bar** to the lower right to move down the page.
8. ☐ Under **Actions,** you can Audit or restrict activities on Windows devices just like you did in the Template. Click on **+ Add an action.**
9. ☐ Click on **Audit or restrict activities on Windows devices** (Note: The actions that have been configured for Windows devices previously.)
10. ☐ Click on the scroll bar on the lower right to move down the page one more time. You can review other rules you have created in the Template version already.
11. ☐ Continue by clicking on the **right scroll bar** on the bottom right to move down the page one more time. Review additional options.
12. ☐ Continue by clicking on the **right scroll bar** on the bottom right to move down the page one more time. Review additional options. We can now move back to finalizing the DLP Device Policy for Contoso.
13. ☐ Click on the **Cancel** button.
14. ☐ In the **Customize advanced DLP rules** section, click **Next**
15. ☐ In the **Define policy settings** section, click on **Review and customize default settings from the template**
16. ☐ In the **Define policy settings** section, click **Next**.
17. ☐ In the **Info to protect** section, click **Next**.

    Note: This will take you back through what you have already created in the template until we submit. So, it will be just a review.

18. ☐ In the **Protection actions** section, click **Next**
19. ☐ In the **Test or turn on the policy** section, if you click on test it out first, you test the policy to ensure it works correctly prior to deploying. Click on the **Yes, turn it on right away** button to validate the DLP policies we will see in Exercise 5.
20. ☐ Click on **Next**.
21. ☐ Review your policy on the **Review your policy and create it** page and click on **Submit**. You should see a **New Policy Created notice.** (Note: After roughly one hour, all the places that you've configured in this policy will begin to enforce the new settings that were applied.)
22. ☐ Click on the **Done** button.
23. ☐ Click on the **Right Scroll Bar** towards the bottom of the page to move down.

24. ☐ You can see the **Contoso EP – PCI Data Security Policy** you have created at the bottom of the page.

Congratulations, you have configured the DLP policy for Endpoint Devices.

Click on the Congratulations Box to move to Exercise 4.

Exercise 4 Validation of the User Experience

This section will show you the experience on a Windows 10 device when users are interacting with the sensitive data subject to the Contoso PCI Data Security Standard (PCI DSS) DLP Policy you just created.

In this exercise, you are Irvin Sayers in the Contoso organization. You will experience what occurs when Irvin, who has been onboarded to the Contoso Group, tries to perform functions with Highly Confidential data that has been identified through previously setting up DLP policies in exercise **3.1 Configuration Using the Template.** You will try to print, copy sections and full files using a PDF Obsidian file and a Microsoft Word Obsidian file. They both contain Highly Confidential information.

Exercise 4.1 – Printing a Confidential PDF File in Edge

1. ☐ In the Windows Desktop, using your **right mouse button**, click on the Project Obsidian PDF file.
2. ☐ With the left mouse button, click on **Open with.**
3. ☐ Select **Microsoft Edge.**
4. ☐ The Obsidian PDF should open. Click on the **Printer icon** at the top right.
5. ☐ On the print page, click on the **Print** button at the bottom left
6. ☐ A dialogue box appears at the top informing you this is a file containing sensitive information and giving you the option to override and print the file if you would like to. (Note: In Exercise 3.1 in the **Audit or restrict activities on Windows devices** section under **Print** you chose to Block with override. Click on the **Cancel** button as we will do nothing at this time and move to the next exercise.

Exercise 4.2 – Copying Data from a Confidential PDF File

1. ☐ While still in the Project Obsidian PDF file you can see that the words **Updated Engine Chip Design** have previously been selected. Click on this selection with the **right mouse button**.
2. ☐ Using the left mouse button click on **Copy**.
3. ☐ A dialogue box appears at the top informing you this is a file containing sensitive information and giving you the option to override and still copy the selection. (Note: In Exercise 3.1 in the **Audit or restrict activities on Windows devices** section under **Copy to**

Clipboard,you chose to Block with override. Click on the **Cancel** button as we will do nothing at this time and move to the next exercise.

4. ☐ Click on the **X** at the top right of the screen to close the Project Obsidian PDF File to move to Exercise 4.3.

Exercise 4.3 – Opening a Confidential PDF File in a third-party browser or application

1. ☐ In the Windows Desktop, using your **right mouse button**, click on the Project Obsidian PDF file.
2. ☐ With the left mouse button, click on **Open with.**
3. ☐ Select **Google Chrome.**
4. ☐ You should see the error that "This site can't be reached". In addition, you will see the Windows Security Data Loss Prevention error dialogue box at the bottom with more details on the policy you created in exercise 3.1, but also Google Chrome was identified as an unallowed browser/ application in exercise 2 on the **Data loss prevention** homepage. Click on the **Dismiss** button at the bottom as we will do nothing at this time and move to the next exercise.
5. ☐ Click on the **X** at the top right of the screen to close this screen to move back to the Windows Desktop to Exercise 4.4.

Exercise 4.4 - Copying Data from a Confidential Microsoft Word File to another Document.

1. ☐ In the Windows Desktop, **Double-Click** on the Microsoft Word icon.
2. ☐ This should load the Microsoft Word Project Obsidian file. The words **Updated Engine Chip Design** have previously been selected. Click on this selection with the right mouse button.
3. ☐ Using the left mouse button click on **Copy** in the dropdown box that appears.
4. ☐ Click on the **Notepad** icon on the taskbar at the bottom of the screen.
5. ☐ In the Notepad application, click on **Edit** at the top.
6. ☐ Click on **Paste** in the drop-down box that appears.
7. ☐ The Windows Security Data Loss Prevention error dialogue box appears at the bottom identifying this is an action that is limited by the DLP policy you created in exercise 3.1. You can still override and copy the selection but will need to provide a business justification. Click on the **Dismiss** button at the bottom as we will do nothing at this time and move to the next exercise.
8. ☐ Click on the **X** at the top right of the file to close Notepad to move to exercise 4.5.

Exercise 4.5 Printing a Confidential Microsoft Word File

1. ☐ Click on **File** at the top left of the Microsoft Word Project Obsidian file.

2. ☐ Click on **Print** on the left.
3. ☐ Under Printer click on the **drop-down** box**.**
4. ☐ Select the **Brother DCP-L2540DW series**
5. ☐ Click on the **Print** button at the top.
6. ☐ The Windows Security Data Loss Prevention error dialogue box appears at the bottom identifying this is an action that is limited by the DLP policy you created in exercise 3.1. You can still override and print the file but will need to provide a business justification. Click on the **Dismiss** button at the bottom as we will do nothing at this time and move to the next exercise.
7. ☐ Click on the **X** at the top right of the file to close the Microsoft Word Project Obsidian file to move to exercise 4.6.

Exercise 4.6 – Copying a Confidential Microsoft Word File to as USB Drive

1. ☐ On the Windows Desktop click on the **Microsoft Word Project Obsidian** file with the Right mouse button.
2. ☐ In the drop-down box, click on **Copy**.
3. ☐ Click on the **Windows File Explorer** icon on the taskbar at the bottom of the screen.
4. ☐ Click on the **USB Drive (D:)**icon on the left with a right mouse click.
5. ☐ Click on **Paste** in the box that appears.
6. ☐ The Windows Security Data Loss Prevention error dialogue box appears at the bottom identifying this is an action that is limited by the DLP policy you created in exercise 3.1 as seen previously. Click on the **Dismiss** button at the bottom as we will do nothing at this time.
7. ☐ Click on the **X** at the top right of the **Windows File Explorer** to close.

Congratulations you have completed Exercise 4 Validation of User Experience

Click on the Congratulations Box to move to Exercise 5

Exercise 5: Review of Data Classification

As a Microsoft 365 compliance administrator, you can evaluate and then tag content in your organization to control where it goes, protect it no matter where it is, and ensure that it is preserved and deleted according to your organization's needs. You do this through the application of sensitivity labels, retention labels, and sensitive information type classification.

The data classification section shows you how out of the box from the moment you have deployed Endpoint DLP to your devices, you get immediate visibility into how and where sensitive data is being used from and on those devices. This includes tools like communication compliance, insider risk management, and data loss prevention.

It can show:

- The number of items that have been classified as a sensitive information type and what those classifications are.
- The top applied sensitivity labels in both Microsoft 365 and Azure Information Protection
- The top applied retention labels
- A summary of activities that users are taking on your sensitive content
- The locations of your sensitive and retained data

This exercise will show some of the telemetry available after DLP policies have been created and subsequently validated through actual individual activity. In this case, we will review a few of the activities identified from Exercise 4 by the user Irvin Sayers.

1. ☐ From the Microsoft 365 compliance center, click on **Data Classification** on the left column. This is the overview page of the **Data Classification** section.
2. ☐ Click on the **Activity Explorer** tab at the top. This shows the various types of activity that occurred between any dates you can specify.
3. ☐ In this case, we will review the activity between 12/8/2020 and 12/15/2020. (Note: You can always specify other dates by clicking on the down arrow to the right of the **Date** tab.) We will dig deeper into the activity during this period. While still in the **Data classification** section, click on the down arrow to the right of the **Activity Filter** tab.
4. ☐ You will need to select 4 checkboxes:
    - ☐ Click on the **File printed** box.
    - ☐ Click on the **File copied to network share** box.
    - ☐ Click on the **File accessed by unallowed apps** box.
    - ☐ Click on the **File copied to clipboard** box.
5. ☐ While still in the **Data classification** section, click on the down arrow to the right of the **Location** tab.
6. ☐ Select the **Endpoint devices** check box. (Note: This box may also include locations such as SharePoint, OneDrive, Teams Chat, or Microsoft Cloud App Security to check if there was any activity there.)
7. ☐ Click on the **scroll bar** on the lower right to move down the page. In the Activity detail list lower on the page, you can see the activity during this period that triggered activity associated with the DLP policy that was created in exercise 3.1. Let's dig deeper into a few of them.
8. ☐ Click on the **checkbox** to the left of the first row for **File accessed by unallowed app**. A dialogue box appears that shows the user IrvinS attempted to access Highly Confidential information in the Project Obsidian.pdf file using an unallowed app. (Note: This gives immediate visibility on the Highly Confidential document, username, the file path of where the data originated from, specific types of sensitive data that were detected in the file when that activity was performed, and other critical data and administrator can use.)
9. ☐ Click on the **scroll bar** on the lower right to move down the page and review additional data. (Note: The unallowed app that triggered the block error was Chrome.exe which was configured in the global endpoint DLP policies that were shown in Exercise 2.)
10. ☐ Click on the **Close** button at the bottom.

11. ☐ Click on the right **scroll bar** on the inside section of the **Activity** listing to move down the activities.
12. ☐ Click to the left of the first **File copied to clipboard** entry. This was the Confidential Project Obsidian Spec.docx that Irvin S tried to copy a section of to Notepad.
13. ☐ Click on the **scroll bar** on the lower right to move down the page and review additional data.
14. ☐ Click on the **Close** button at the bottom.
15. ☐ Click on the right **scroll bar** on the inside section to move down the **Activity** listings once more.
16. ☐ Click to the left of the first **File printed** row. IrvinS tried to print the Confidential Project Obsidian Spec.docx. The printer is described, IrvinS's IP address, and other details about the issue.
17. ☐ Click on the **scroll bar** on the lower right to move down the page and review additional data. It shows that it was a Microsoft Word file.
18. ☐ Click on the **Close** button at the bottom.
19. ☐ Click on **Home** at the top left to take you back to the Microsoft 365 compliance center Welcome page.

Congratulations, you have completed Exercise 5 – Review of Data Classification

Summary

To comply with business standards and industry regulations, organizations must protect sensitive information and prevent its inadvertent disclosure. Sensitive information can include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records.

This Interactive Guide has shown you how to better turn on controls to protect the sensitive data that is exploding and expanding across your organization. As users collaborate and produce more and more sensitive content, you must have the right controls to give you that visibility, understand where and how it's being used, and put in those proactive policies to restrict activity that could affect your organization. With a data loss prevention (DLP) policy in the Microsoft 365 compliance center, you can identify, monitor, and automatically protect sensitive information across Office 365.

Additional Resources:

This Interactive Guide walked you through configuring and validating the Data Loss Prevention policy for Windows devices. Here is another interactive guide: DLP for Teams that takes you through setting up DLP policies for the Microsoft Teams chat and channel messages location.