



Microsoft Information Protection

Labs Day 2

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2019 Microsoft. All rights reserved

Contents

Demo Overview: Microsoft Information Protection	4
Intended Audience	4

Demo Prerequisites	4
One-Time Demo Environment Setup.....	Error! Bookmark not defined.
Demo Personas	4
Configure Sensitivity Labels and DLP Policy	4
Pre-demo Setup Steps	5
Unified sensitivity label management in Security & Compliance Center	5
Configure Office 365 Data Loss Prevention in Security & Compliance Center	6
Reset Steps	7
Native Sensitivity Labeling in Office Apps Across Platforms (Click-through-guide only).....	8
Pre-demo Setup Steps	8
Labeling in Office for Mac (Click-through-guide).....	8
Office mobile apps for iOS (Click-through-guide)	9
Office on Windows (Click-through-guide).....	10
Send a Protected Email to an External User	10
Pre-demo Setup Steps	10
Send Protected Email to a Gmail User	10
Prevent Sharing of Sensitive Data with Office 365 Data Loss Prevention	11
Pre-demo Setup Steps	12
Block sharing of sensitive information from SharePoint Online	12
Block sharing of sensitive information from Teams	13
Reset Steps	14
Protect Sensitive Files in 3rd Party Cloud Services (Click-through-guide only).....	14
Pre-demo Setup Steps	14
Labeling documents in a 3rd party cloud service	14
Protect Sensitive Information on Windows 10 Devices (Click through guide only)	15
Pre-demo Setup Steps	15
Block copying and moving sensitive files on Windows 10 devices.....	15
Appendix: Set up the Demo Tenant	17
Add authentication phone and email to the demo user persona	17
Configure a Data Loss Prevention (DLP) Policy	17
Set up an External Email Account for Office 365 Message Encryption	18
Set up a Gmail Account.....	18

Lab Overview: Microsoft Information Protection

The growth and mobility of data, across devices, apps, cloud services and on-premises, has made protecting sensitive information more challenging than ever. Internal security requirements and evolving compliance regulations have heightened the importance on implementing a comprehensive information protection strategy. Microsoft Information Protection enables you to protect your sensitive information, wherever it lives or travels, across devices, apps, cloud services and on-premises.

Our solution leverages the power of its unified platform to protect and manage sensitive data across its lifecycle: Discover and understand where sensitive information resides; classify & label files and emails based on sensitivity; apply protection based on flexible policies; and monitor your sensitive data landscape for potentially risky or undesirable activity. Microsoft Information Protection solutions are easy for IT admins to configure and manage, and they provide comprehensive analytics to better understand your sensitive data landscape and take corrective action. Protection capabilities are built natively into productivity apps and services, giving end-users a consistent and simple approach to securing their information, without inhibiting their productivity.

Microsoft Information Protection refers to a set of products and integrated capabilities. Individual products and capabilities that are typically included as part of the Microsoft Information Protection discussion are Azure Information Protection, Office 365 Information Protection (e.g. Office 365 DLP), Windows Information Protection and specific capabilities in Microsoft Cloud App Security.

Intended Audience

Security IT admins, CISOs

Lab Pre-requisites

1. Please ensure you have access to Partner Center. If you have not got access please follow the “Getting Started Guide” which can be downloaded here <https://aka.ms/m365masterclass-Intro>
2. If this is the first time completing this lab please go to [Appendix: Set up the tenant for this lab](#)

Lab Personas

The recommended lab personas to use for in this guide, unless otherwise stated, are:

- Administrator scenarios: admin@<tenant>.onmicrosoft.com
- End user scenarios (Hero User): Isaiah Langer, IsaiahL@<tenant>.onmicrosoft.com

The default password for both users can be found on your tenant information card at <https://demos.microsoft.com>.

- Create a Gmail account to be used for the Send Protected Message to a Gmail User and Block sharing of sensitive information from SharePoint Online scenarios.

Microsoft Information Protection

Configure Sensitivity Labels and DLP Policy

Use Azure Information Protection or Office 365 to setup your sensitivity labels and protection policies to protect sensitive documents and email. Configure data loss prevention policies to block the accidental or inappropriate sharing of sensitive information.

Pre-lab Setup Steps

Carry out these setup steps prior to each demonstration:

1. Launch an InPrivate Microsoft Edge browser session and navigate to <https://protection.office.com>. Sign in as admin@<Tenant>.onmicrosoft.com using the tenant password from demo card on demos.microsoft.com.

Talking Points	Click Steps
<p>Unified sensitivity label management in Security & Compliance Center</p> <p>In this scenario, the admin will create a new sensitivity label that will be used to protect confidential information.</p> <p>You can create an encryption policy immediately while creating the label or add it later.</p> <p>The admin will select to encrypt email messages and files, as well as give permissions to users and groups.</p> <p>Only the users and groups selected will be assigned permissions to use the content that has this label applied.</p> <p>The admin will search for a group and select Project Falcon.</p> <p>After encryption has been configured, the content will be marked and managed.</p> <p>Enabling content marking you can add custom headers, footers, and watermarks to the content that has this label applied.</p>	<ol style="list-style-type: none"> 1. In the Security & Compliance portal, in the left-hand navigation, click Classifications. 2. Click Labels. 3. At the top, click Create a label. 4. On the Name your label page, create a label as follows: <ul style="list-style-type: none"> • Label name: Confidential-PCI • Tooltip: This content contains sensitive personal information 5. Click Next. 6. Define Scope → Files and Emails 7. Under Protection setting, select Encrypt files and email and mark the content of files 8. Under Encryption, → Encrypt 9. Under Grant permissions to specific users and groups, click Assign permissions. 10. Click + Add users or groups. 11. On the Add users or groups page, click + Add. 12. In the Search text box, type Project, click Project Falcon, and then click Add. 13. On the Add users and groups page, click Done. 14. On the Assign permissions page, click Save. 15. On the Encryption page, click Next. On the Content marking page, click On to enable.

Next to Add a watermark, click the check box, and then click Customize text.

<p>After content marking has been configured, you'll manage data loss prevention on the endpoint, specifically Windows 10 machines.</p> <p>During the final review of the settings, you can edit specific settings or choose to create the label.</p> <p>After the label is created, settings can still be edited, the label can be published or deleted.</p> <p>Now that the label has been creating and configured, it can be applied automatically or by the user, and the content will be protected based on the settings configured.</p>	<ol style="list-style-type: none"> 16. In the Watermark text field, type CONFIDENTIAL, and then click Save. 17. On the Content marking page, click Next. 18. On the Auto labeling page, click On to enable. 19. Under Detect content that contains, click + Add a condition, and then click Content contains. 20. Under Content contains, click the Add drop-down list, and then click Sensitive info types. 21. On the Sensitive info types page, click + Add. Select Sensitive info types as follows: <ul style="list-style-type: none"> Credit Card Number U.S. /U.K. Passport Number U.S. Bank Account Number U.S. Driver's License Number U.S. Individual Taxpayer Identification Number (ITIN) U.S. Social Security Number 22. Click Add. 23. On the Sensitive info types page, verify the options and click Done. 24. On the Auto labeling page, click Next. 25. On the Review your settings page, verify the options selected, and click Create. 26. 27. 28.
<p>Configure Office 365 Data Loss Prevention in Security & Compliance Center</p> <p>To comply with business standards and industry regulations, organizations need to protect sensitive information and prevent accidental oversharing and leakage.</p> <p>With an Office 365 data loss prevention (DLP) policies, you can prevent the inappropriate sharing of sensitive information.</p>	<ol style="list-style-type: none"> 1. In the Security & Compliance portal, in the left-hand navigation, click Data loss prevention. 2. Click Policy. 3. Click + Create a policy. 4. On the Start with a template or create a custom policy page, click Privacy, click General Data Protection Regulation (GDPR), and then click Next.

<p>The admin will use the General Data Protection Regulation (GDPR) template, to create a DLP policy to identify personal information inside the European Union (EU).</p> <p>Using a DLP policy, you can:</p> <ul style="list-style-type: none"> • Detect sensitive information across many locations, including email in Exchange Online, and documents in SharePoint Online and OneDrive for Business, and in the desktop versions of Excel, PowerPoint, Word and Outlook. • Prevent the accidental sharing of sensitive information. • Monitor policy violations for further investigation. • Help users learn how to stay compliant without interrupting their workflow with notifications and “policy tips”. <p>A DLP policy contains a few basic settings:</p> <ul style="list-style-type: none"> • Where to protect the content - locations such as Exchange Online, SharePoint sites, and OneDrive accounts, and Microsoft Teams chats. • Conditions for applying policy, such as a match against one of the over 90 sensitivity information types, or your own custom sensitive information types. • When and how to protect the content by enforcing rules. <p>After you have created the policy, you have the option of turning on the policy or testing it first.</p>	<ol style="list-style-type: none"> 5. On the Name your Policy page, review the defaults and click Next. 6. On the Choose locations page, click Let me choose specific locations, and then click Next. 7. On the Choose locations page, review the locations, and point out Teams chat and channel messages. 8. Click Next. 9. On the Customize the type of content you want to protect page, click Use advanced settings, and then click Next. 10. On the Customize the type of content you want to protect page click Low volume EU Sensitive content found. 11. Click Edit rule. 12. On the Low volume EU Sensitive content found configure the settings as follows: <ul style="list-style-type: none"> • Conditions > Content is shared: with people outside my organization • Actions > +Add an action > Restrict access or encrypt the content: Block people from sharing and restrict access to shared content / Only people outside your organization. People inside your organization will continue to have access. 13. Click Save. 14. On the Customize the type of content you want to protect page, click Next. 15. On the Do you want to turn on the policy or test things out first click Yes, turn it on right away and click Next. 16. On the Review your settings page, verify the options selected, and click Create. 17. On the General Data Protection Regulation page, click Close.
---	---

Reset Steps

1. **In the Security & Compliance portal, delete the Confidential – PCI label.**
 - a. **In the Security & Compliance portal, in the left-hand navigation, click Classifications.**
 - b. **Click Labels.**

- c. **Click the Confidential – PCI label to view the details fly-out.**
- d. **On the Confidential – PCI fly-out, click Delete label, and then click Yes.**

Native Sensitivity Labeling in Office Apps Across Platforms (Click-through-guide only)

Microsoft is improving the information protection experience for its end-users by making it easy to add sensitivity labels to their documents and emails. The easier it is to do, the more likely they are to classify information correctly. We are building sensitivity labeling into Office apps across platforms, including Mac, iOS, Android and Windows.

Pre-Lab Setup Steps

1. **Open the click through guide PowerPoint file for Microsoft Information Protection, downloaded from <https://demos.microsoft.com>.**

Speaker Script	Click Steps
<p>Labeling in Office for Mac (Click-through-guide)</p> <p>In Office apps on Mac (Word, PowerPoint, Excel and Outlook), sensitivity labels appear on the Sensitivity button, on the Home tab, and on the Ribbon. The label applied also appears in the Status bar at the bottom of the window. After a sensitivity label is applied to an email or document, the protection settings for that label are enforced on the content.</p> <p>Let's review the end user experience starting with a Mac. When collaborating with your colleagues on a document using your corporate MacBook, you're going to use Office for Mac.</p> <p>You've added details about a fundraiser that you're planning, and you know your company has policies to classify and apply the correct sensitivity label to any document, even if it doesn't contain sensitive data.</p> <p>Right within Word on Mac, you can use the new, built-in label picker to easily select the right label that's appropriate for this document. Using the Sensitivity drop-down menu, you can apply the "Highly Confidential" label.</p> <p>The sensitivity label is applied to the document, and the Highly Confidential watermark is also added to the document.</p> <p>Next, we'll review how this works in Excel.</p>	<ol style="list-style-type: none"> 1. Click the Word icon (bottom right) to maximize. 2. In the top-right corner, click Sensitivity. 3. Click Highly Confidential label from drop-down. 4. Click the Excel icon (bottom right) to maximize.

<p>Similar to Word, in Excel, you can use the new, natively integrated label picker to easily select the right label that's right for this document. Using the drop-down menu, you can apply "Confidential-Finance" label.</p> <p>The sensitivity label is added to the document's properties.</p> <p>The new, natively integrated label picker to easily select the right label is now available in Outlook for email also. Using the drop-down menu, you can apply the "Highly Confidential" label.</p> <p>When this email is sent, the receiver will see that the email is protected. The header of the email contains information indicating that it is Confidential. The header information displayed can be customized by IT admins.</p>	<ol style="list-style-type: none"> 5. In Excel, click Sensitivity (top-right corner). 6. Click the Confidential-Finance label. 7. Click the Outlook icon (bottom right) to maximize. 8. Click Sensitivity. 9. Click Highly Confidential. 10. Click Send.
<p>Office mobile apps for iOS (Click-through-guide)</p> <p>In Office apps on iOS devices, sensitivity labels appear on the Sensitivity button, on the Home tab on the Ribbon. The applied label also appears in the Status bar at the bottom of the window.</p> <p>Let's review the end user experience on iOS. The Sensitivity button allows you to apply the different labels. As you apply different sensitivity labels, the watermark reflects the label selected.</p> <p>Selecting a Sensitivity label is the same across apps on a platform. When using PowerPoint, you see the same sets of labels as you did in Word. Initially the document has no labels applied.</p> <p>When a label is applied, the appropriate watermark and permissions are applied.</p>	<ol style="list-style-type: none"> 11. Click Confidential-Finance. 12. Click the screen to advance the slide and show PowerPoint. 13. In PowerPoint, click the 2nd slide. 14. Click Sensitivity. 15. Click Highly Confidential. 16. Click the screen to advance the slide, and show the watermark applied for the sensitivity label. 17. Click the screen to advance the slide and zoom in on the watermark.
<p>Office mobile apps for Android (Click-through-guide)</p> <p>In Office apps on Android devices, sensitivity labels appear on the Sensitivity button, on the Home tab, and on the Ribbon. The label applied also appears in the Status bar at the bottom of the window.</p> <p>Labels are applied very consistently across platforms. No matter what platform you're using, the appropriate permissions and watermarks will be applied.</p>	<ol style="list-style-type: none"> 18. Click Highly Confidential. 19. Note that the watermark has been applied.

<p>Office on Windows (Click-through-guide)</p> <p>In Office apps on devices running Windows, sensitivity labels appear on the Sensitivity button, on the Home tab, and on the Ribbon. The label applied also appears in the Status bar at the bottom of the window.</p> <p>Let's review the sensitive labels for applications in Windows:</p> <ul style="list-style-type: none"> • Outlook • Excel • Word <p>This demonstrates that you can consistently use and apply sensitivity labels for users across all your platforms.</p>	<p>20. Click the screen to advance the slide and show Outlook.</p> <p>21. Click the screen to advance the slide and show Excel.</p> <p>22. Click the screen to advance the slide and show Word.</p>
---	--

Send a Protected Email to an External User

People often use email to exchange sensitive information, such as financial data, legal contracts, confidential product information, sales reports and projections, patient health information, or customer and employee information. As a result, mailboxes can become repositories for large amounts of potentially sensitive information, and information leakage can become a serious threat to your organization.

Office 365 Message Encryption enables users to send protected email messages to people inside and outside the organization. Protected emails easily work with users across a variety of services, including Office 365, Outlook.com, Gmail, Yahoo, and other email services.

Recipients can read and respond to messages protected by Office 365 Message Encryption no matter what email provider they use.

Pre-demo Setup Steps

1. Launch an InPrivate session in the web browser and navigate to <https://portal.office.com>.
2. **Sign in as** IsaiahL@<tenant>.onmicrosoft.com **using the tenant password from demo card on** demos.microsoft.com. **Minimize the web browser.**
3. **On the Office 365 portal, click Outlook.**
4. **Click The new Outlook, when prompted.**
5. **On a new browser tab, navigate to** <http://gmail.com>. **Sign in as the Gmail user created in the pre-demo steps.**

Speaker Script	Click Steps
Send Protected Email to a Gmail User	

Speaker Script	Click Steps
<p>Isaiah needs to communicate with a PR firm about an upcoming ad campaign at Contoso. The PR firm uses Gmail as their email provider.</p> <p>You can create policies that enforce encryption on all email messages sent to external recipients, so when a new message is composed to an external recipient, it is automatically protected.</p> <p>For this scenario, Isaiah will manually encrypt the email being sent to an external recipient.</p> <p>Gmail is not RMS-aware, so when Alex receives the message, it's wrapped in another email that provides instructions on how to read it.</p> <p>Because Alex is using Gmail, he has the option of using the new federated sign-in experience to read this message. When he signs in with his Gmail credentials, the message is displayed.</p> <p>And no matter what email provider the recipient uses, they can always read an encrypted message by requesting a one-time key.</p>	<ol style="list-style-type: none"> Switch to the browser tab with Isaiah's email account open. NOTE: Verify The new Outlook is selected to ensure the scenario works as written. Click +New message. In the To line, type the external Gmail address created during setup. In the Subject line, type Project opportunity. Click the Attachment icon (📎). Click Cloud locations. Select European Expansion.xlsx and click Next. Click Attach as a copy. In the message body, type Are you available to work on a new campaign? Click on (...) --> Encrypt On the Encrypt, click Encrypt-Donot Forward. Click Send. Switch to the web browser tab with the external Gmail account open. Click on the new message from Isaiah Langer. Click Read the message. If required, click Sign in with Google and follow the sign in steps. In the email, click European Expansion.xlsx.

Prevent Sharing of Sensitive Data with Office 365 Data Loss Prevention

To comply with business standards and industry regulations, organizations need to protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII), such as credit card numbers, social security numbers, or health records. With a Data Loss Prevention (DLP) policy in the Office 365 Security & Compliance Center, you can identify, monitor, and automatically protect sensitive information across Office 365.

With a DLP policy, you can:

- Identify sensitive information across many locations, such as Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams.
- Prevent the accidental sharing of sensitive information.
- Monitor and protect sensitive information in the desktop versions of Excel, PowerPoint, and Word.
- Help users learn how to stay compliant without interrupting their workflow.
- View DLP reports showing content that matches your organization's DLP policies.

Pre-lab Setup Steps

- 1. Configure browser sessions for Isaiah Langer:**
 - a. Launch an InPrivate session in the web browser and navigate to <https://portal.office.com>.
 - b. Sign in as IsaiahL@<tenant>.onmicrosoft.com using the tenant password from demo card on demos.microsoft.com.
 - c. On the Office 365 portal, click OneDrive and Teams. OneDrive and Teams will open in separate tabs.
 - d. On the Teams tab, click Use the web app instead.
 - e. On the browser with Teams open, in left hand navigation, click Chat, and then click Allan Deyoung.
- 2. Configure browser session for Allan Deyoung:**
 - a. Launch an InPrivate session in the web browser and navigate to <https://portal.office.com>.
 - b. Sign in as AllanD@<tenant>.onmicrosoft.com using the tenant password from demo card on demos.microsoft.com.
 - c. On the Office 365 portal, click Teams. Teams will open in separate tabs.
 - d. On the Teams tab, click Use the web app instead.

Speaker Script	Click Steps
<p>Block sharing of sensitive information from SharePoint Online</p> <p>Data loss prevention in Office 365 helps organizations protect their sensitive data across their Office 365 environment, including Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams.</p> <p>Contoso has strict requirements to protect various types of data for regulatory, policy, or privacy reasons. They use Office 365 Data Loss Prevention policies to help achieve this goal.</p>	<ol style="list-style-type: none"> 1. Switch to the browser, with OneDrive open. 2. Click to the left of Contoso Purchasing Permissions -Q1.docx.

Speaker Script	Click Steps
<p>For example, when Isaiah Langer accesses his OneDrive for Business folders, he sees this icon on a document he owns.</p> <p>This warning tells him that this document has been flagged by a DLP policy. In this case, the document has been flagged because it contains credit card information.</p> <p>Isaiah wants more information, so he looks at the document properties. Here he can get more information. He can also report this to an administrator if he thinks the policy is been applied in error.</p> <p>When Isaiah tries to share the content, he is informed that the item contains sensitive information and can't be share outside the organization.</p>	<ol style="list-style-type: none"> 3. In the upper right corner, click the information icon, and review the policy information. 4. Click View policy tip and review the reason the label was applied. 5. Click X to close the policy tip. 6. Click Share. 7. In Enter a name or email address, type the Gmail address, and then click the email address when it is verified. 8. Note the message informing that the item contains sensitive information and can't be shared with people outside your organization. 9. Click X to close Share Link.
<p>Block sharing of sensitive information from Teams</p> <p>Data loss prevention (DLP) has been available for Exchange Online, SharePoint Online and OneDrive for Business for a while, and DLP has been recently extended to Microsoft Teams, to enable the blocking of sensitive information contained in chat messages and channel conversations.</p> <p>This is based on the same policy engine used and proven in our other DLP services.</p> <p>When someone sends a message, either within a chat or a channel, the content of the message is inspected for sensitive information in near real-time. If sensitive information is identified, then the message is revoked and no longer accessible by the recipient(s).</p> <p>Similar to how DLP operates in other Office 365 services, policy tips give the sender additional information on the reason for the message being blocked, such as the presence of passport information or social security numbers.</p>	<ol style="list-style-type: none"> 10. Switch to the browser with Teams open. 11. In the chat with Allan Deyoung, type EU Passport number x13256730, and then click Send. 12. Note the message, This message was blocked.

Speaker Script	Click Steps
<p>End-users can override the blocked message or report the issue as a false positive, if allowed by IT.</p> <p>For organizations that are using Microsoft Teams to accelerate their workforce collaboration and productivity, this provides a new way to ensure proper control and governance of important data – both for the purpose of achieving internal security objectives as well as meeting external compliance and privacy requirements.</p>	<p>13. Switch to the browser window with Teams signed in with Allan Deyoung.</p> <p>14. Note the blocked message from Isaiah.</p>

Reset Steps

1. **In the Security & Compliance portal, delete the General Data Protection Regulation data loss prevention policy.**
 - a. **In the Security & Compliance portal, in the left-hand navigation, click Data loss prevention.**
 - b. **Click Policy.**
 - c. **Click the General Data Protection Regulation (GDPR) policy to view the details fly-out.**
 - d. **On the General Data Protection Regulation (GDPR) fly-out, click Delete policy, and then click Yes.**

Protect Sensitive Files in 3rd Party Cloud Services (Click-through-guide only)

More and more data lives in cloud services and SaaS apps. With Microsoft Information Protection solutions, you can easily discover, classify, label and protect sensitive information that resides in cloud services. This leverages the same classification methods and sensitivity labels used in our other information protection services.

Pre-lab Setup Steps

1. **Open the click-through guide PowerPoint file for Microsoft Information Protection, downloaded from <https://demos.microsoft.com>.**

Speaker Script	Click Steps
<p>Labeling documents in a 3rd party cloud service</p> <p>Isaiah's team is using a cloud storage service, such as Box, to store and share some of their confidential documents. Azure Information Protection and Microsoft Cloud App Security work together to discover, classify & label, protect and monitor files that reside in third party cloud services.</p> <p>You can create a file policy using Microsoft Cloud App Security, that enables content with specific key words or sensitivity information types to be labeled and protected.</p>	<ol style="list-style-type: none"> 1. Switch to the click-through-guide. 2. Review the file policy and the following options: <ul style="list-style-type: none"> • Create a filter for the files this policy will act on • Content Inspection Method 3. Click the policy to scroll down. 4. Under Governance, in the Box section, review: <ul style="list-style-type: none"> • Apply classification label

Speaker Script	Click Steps
<p>When a file is uploaded to a 3rd party service, like Box, that contains the key words or matches sensitive information types, the label will be automatically applied. As you see, V2 is appended to the document name indicating that the file has been labeled and protected, including restricting permissions on who can access the file.</p> <p>Back in Microsoft Cloud App Security, you'll see that the document is listed as matching the policy that you created.</p> <p>Azure Information Protection and Microsoft Cloud App Security work together to help protect sensitive information, even if it is stored in cloud services.</p>	<ul style="list-style-type: none"> • Select an Azure Information Protection classification label to be used to protect matching files <ol style="list-style-type: none"> 5. Click to switch to the browser tab with Box open. 6. Review the files uploaded. 7. Click to "refresh" the screen and note the V2 by the document name. 8. Click to switch back to Microsoft Cloud App Security, Info Protection Demo Policy and review the files. 9. Click Confidential Document, to show details for the file. 10. Review the details for the file.

Protect Sensitive Information on Windows 10 Devices (Power Point Labs day 2 guide only)

Protecting sensitive information is no longer limited to on-premises devices that are centrally managed and controlled. More and more, company data also resides on personal PCs and devices owned by employees. Windows Information Protection helps protect sensitive data on Windows 10 devices against accidental leakage through apps, cloud services, and social media.

Pre-lab Setup Steps

1. **Open the click through guide PowerPoint file for Microsoft Information Protection, downloaded from <https://demos.microsoft.com>.**

Speaker Script	Click Steps
<p>Block copying and moving sensitive files on Windows 10 devices</p> <p>Isaiah works in the Sales & Marketing department at Contoso. He often takes his files offline to work on at home or while travelling.</p> <p>Windows understands sensitivity labels in documents and can use that information to enforce policy. This file in OneDrive is labeled as Confidential.</p>	<ol style="list-style-type: none"> 1. Begin the demo in OneDrive in the browser. 2. Under Files, click European Fashion Lines 3. Next to the file European Fashion Lines.docx, click the vertical ellipsis. 4. Click Open and then click Open in Word. 5. In Word, point out the Confidential label and the Confidential watermark.

Speaker Script	Click Steps
<p>When Isaiah downloads this document from the Contoso OneDrive, Windows Information Protection policy is enforced based on this sensitivity labels, which means blocking or controlling the copying or transfer of information from this labeled document to other apps and locations on the device.</p> <p>Isaiah finds some of this information exciting and wants to share some of it with his followers on Twitter. He opens the document using Microsoft Word, which is an approved work app. Note that the downloaded file, still has the Confidential label, as it did in OneDrive.</p> <p>He copies the text and then tries to paste it into a new tweet.</p> <p>Windows Information Protection prevents him from doing so because of the sensitivity label in the document, and it gives him a reminder that this is privileged business information.</p> <p>If Isaiah thinks this is a reasonable use of business information, he can go ahead and allow it to be pasted. Isaiah thinks better of this and cancels the Tweet. Contoso could also configure this policy to simply block the copy and paste altogether.</p> <p>Contoso can also use Windows Information Protection to ensure that labeled and protected files preserve their protection when being copied to removable storage, like a USB drive, or block copying to cloud locations, such as OneDrive for Business or other cloud repositories.</p>	<ol style="list-style-type: none"> 6. Click X to close Word. 7. In OneDrive, next to the file European Fashion Lines.docx, click the vertical ellipsis. 8. Click Download. 9. At the bottom, to the right of Save, click the up arrow. 10. Click Save as. 11. In the Save As window, browse to the Documents folder and click Save. 12. At the bottom of the browser, click Open Folder. 13. Double-click to open European Fashion Lines. 14. Point out the Confidential label and the Confidential watermark. 15. Scroll down to the second page. 16. Highlight some text on the page, right-click, and then select Copy. 17. On the taskbar, click the web browser and switch to the tab with Twitter already open and logged in. 18. Click What's happening? to start a new tweet. 19. In the text box, right click and select Paste. 20. In the Use work content here? text box, point out the warning that appears, and then click No.

Appendix: Set up the tenant for this lab

When using a lab environment provisioned through demos.microsoft.com, the tenant is already equipped with appropriate trial licenses for the underlying products and populated with relevant content. Configuration or validation of policy settings is still required, as described below. These steps need to be performed only once per demo environment.

Add authentication phone and email to the demo user persona

The recommended hero user persona for most scenarios documented here is Isaiah Langer (IsaiahL@<tenant>.onmicrosoft.com). Configure this user with a second-factor authentication option:

1. **Open a new In Private browser session (In Microsoft Edge, CTRL + SHIFT + P).**
2. **Sign in to <https://myapps.microsoft.com> portal as IsaiahL@<tenant>.onmicrosoft.com. The password for this user can be found on demo card at demos.microsoft.com.**
3. **Click the user icon menu (top-right corner), then select Profile.**
4. **Click Set up self-service password reset.**
5. **Follow the on-screen prompts to set up Authentication Phone and Authentication Email. Provide a real-world mobile phone number and a real-world email address.**
6. **Click finish when completed.**

Configure a Data Loss Prevention (DLP) Policy

To demonstrate Data Loss Prevention, configure a policy to identify and protect sensitive financial information. The policy might take up to 1 hours to available in the demo:

1. **Open a new InPrivate browser session (In Microsoft Edge, CTRL + SHIFT + P).**
2. **Sign in to <https://protection.office.com> portal as admin@<tenant>.onmicrosoft.com. The password for this user can be found on demo card at demos.microsoft.com.**
3. **In the Security & Compliance portal, in the left-hand navigation, click Data loss prevention.**
4. **Click Policy.**
5. **Click + Create a policy.**
6. **On the Start with a template or create a custom policy page, click Financial, click U.S. Financial Data, and then click Next.**
7. **On the Name your Policy page, review the defaults and click Next.**
8. **On the Choose locations page, click Next.**
9. **On the Customize the type of content you want to protect page, click Use advanced settings, and then click Next.**
10. **On the Customize the type of content you want to protect page, click Low volume of content detected U.S. Financial.**
11. **Click Edit rule.**

12. **On the Low volume of content detected U.S. Financial page, configure the settings as follows:**
 - **Actions > +Add an action > Restrict access or encrypt the content > Block people from sharing and restrict access to shared content / Only people outside your organization.** People inside your organization will continue to have access.
13. **Click Save.**
14. **On the Customize the type of content you want to protect page, click Next.**
15. **On the Do you want to turn on the policy or test things out first, click Yes, turn it on right away, and then click Next.**
16. **On the Review your settings page, verify the options selected, and click Create.**
17. **On the U.S. Financial Data page, click Close.**

Set up an External Email Account for Office 365 Message Encryption

To demonstrate Office 365 Message Encryption (OME), set up an external Gmail account:

Set up a Gmail Account

1. **Navigate to the home page for Gmail:** <https://gmail.com>.
2. **Follow the instructions to create a new email account in the name of Alex Wilber. A cell phone number may be required for verification.**