



Data Classification and Protection with Microsoft Information Protection

(2021 Updates for LAN Administrators)

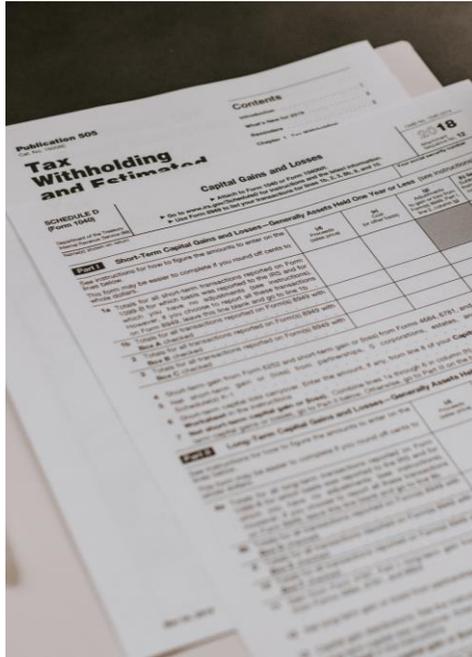
Information Technology Services Centre
December 2020

Agenda

- The Need for Document Protection
- Microsoft Information Protection
- Migration from Classic Client to Unified Client

The Need for Document Protection

- Maintaining high levels of document security keeps the University from loss of intellectual property, damage in reputation and facing legal consequences.



The Need for Document Protection

- [Data Classification and Data Governance Policy](#), published in Aug 2016, proposes a comprehensive framework for protecting University's digital information, particularly digital-based documents.

Level	Data Classification	Definition	Example
1	Strictly Confidential	The HIGHEST level of security controls. Unauthorized disclosure of this data would cause severe adverse effect to individuals or on operations, assets and reputation of the University. <i>The STRICTEST security policy should be applied even if this may incur considerable inconvenience to the users.</i>	<ul style="list-style-type: none">• Data deemed highly confidential by the University• Data protected by regulations such as the Hong Kong Personal Data (Privacy) Ordinance• Health/Patient information may or may not be regulated by Hospital Authority (HA)
2	Confidential	Unauthorized disclosure of this data would cause a moderate level of risk to individuals or the University. <i>Strict security policy should be applied even if this may incur some inconvenience to the users.</i>	<ul style="list-style-type: none">• Data deemed confidential by the University• Personal data (e.g. Student ID, staff ID) not classified as Level 1.

Microsoft Information Protection



Microsoft Azure Information Protection (AIP)

- A **data protection solution** which helps you to classify, label and protect the documents according to the confidential level of the information.
- Once a document is **classified and labelled**, corresponding predefined **security policy will be applied immediately** to protect the document and **limit the access against unauthorized person**.

AIP Supported Document Types

Document Type	Create / Open Protected Document	
Microsoft Office (.docx / .xlsx / .pptx)	Office 2016 <ul style="list-style-type: none">• Use AIP client	Office 2019 & Office 365 <ul style="list-style-type: none">• Use AIP client add-in• Office built-in capability ^{1,2}
PDF	Use AIP client	
Email	Office 2016 <ul style="list-style-type: none">• Use AIP client add-in• Use Outlook on the web ²	Office 2019 & Office 365 <ul style="list-style-type: none">• Use AIP client add-in• Office built-in capability ^{1,2}• Use Outlook on the web ²

¹ Sign-in to Office app required.

² Starting 7 Jan 2021.

Installing AIP Client

- Download the installer from [ITSC Website](#)

Microsoft Information Protection (MIP)

To cope with the Data Classification and Data Governance Policy for protecting University's digital information, an information protection system with **Microsoft Information Protection – MIP**, (formerly Azure Information Protection-AIP and Rights Management Service – RMS), is implemented for protecting digital information according to the defined data class.

Available to
All Staff

Service Charge and Application
Free; no application required

Service Availability
Office hours

Support
Please submit to ITSC Service Desk, Information Security > General Enquiry

- > 1. Policy Background
- > 2. Microsoft Information Protection (MIP) Implementation
- > 3. User Manuals and Briefing Sessions
- ▼ 4. Installation Files
- > 5. FAQ

For standalone installation:

- For standalone installation, you may download and extract the "AzInfoProtection_UL.exe" at <https://www.microsoft.com/en-us/...>

For central deployment:

- For central deployment, you may download and extract the "AzInfoProtection_UL_MSI_for_central_deployment.msi" at <https://www.microsoft.com/en-us/...>



AzInfoProtection_UL.exe

Major Projects | IT Policies | Application Forms | User Guides | Privacy Policy | Disclaimer | Sitemap

 香港中文大學
The Chinese University of Hong Kong

© 2021 All Rights Reserved. The Chinese University of Hong Kong.

Predefined Classification Labels and Visual Markings

- Make your documents compliant with the policy in 1 click.

The image shows a Microsoft Word interface with the following elements:

- 1. Select the classification label:** A callout box points to the 'Sensitivity' icon in the ribbon, which is highlighted with a red box.
- 2. Classification Label applied to the document:** A callout box points to the 'Confidential \ All Staff' label in the ribbon, which is highlighted with a red box.
- 3. Visual Marking added in document header:** A callout box points to the 'Confidential' text in the document header, which is highlighted with a red box.

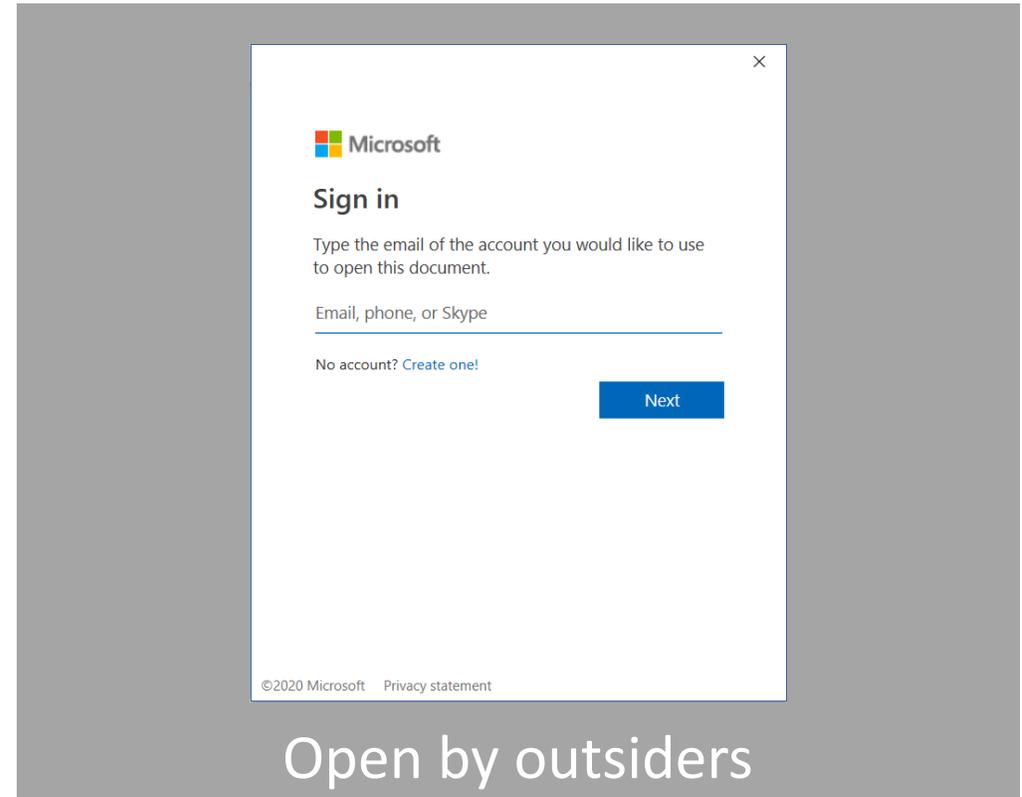
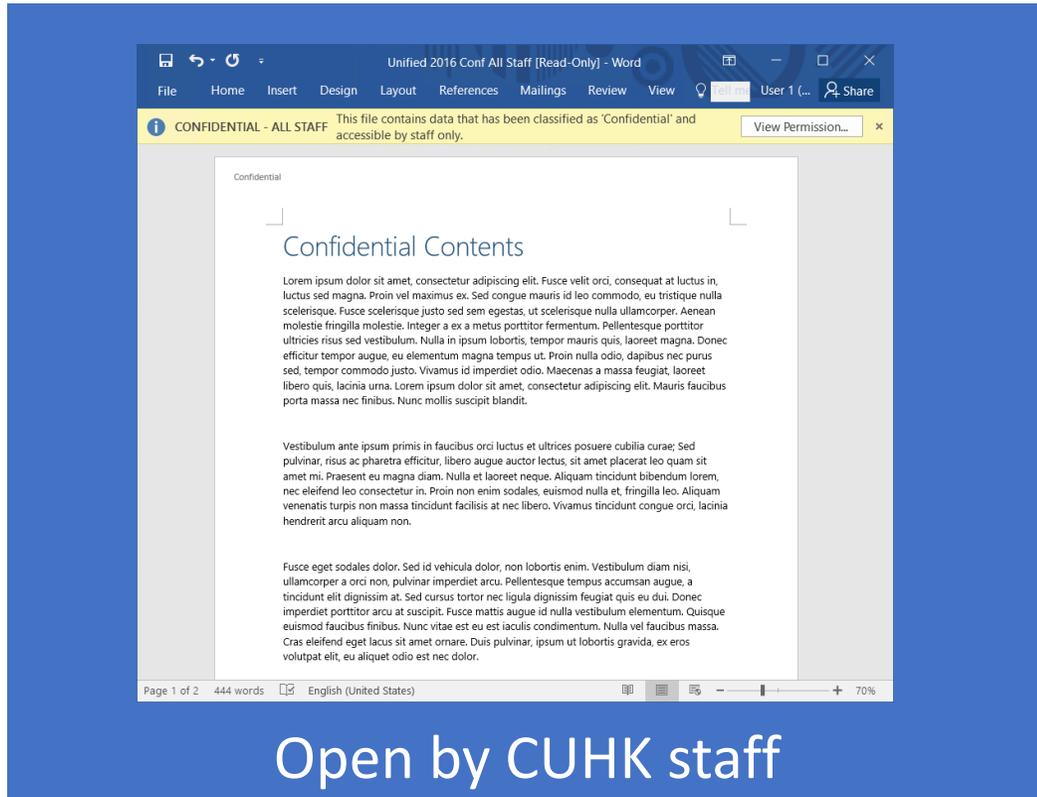
The 'Sensitivity' dropdown menu is open, showing the following options:

- Confidential
- Strictly Confidential
- Show Bar
- Help and Feedback

The 'All Staff' label is also visible in the ribbon.

Open Protected Documents

- Outsiders are unable to open protected documents as they are encrypted.



Predefined Classification Labels and Visual Markings

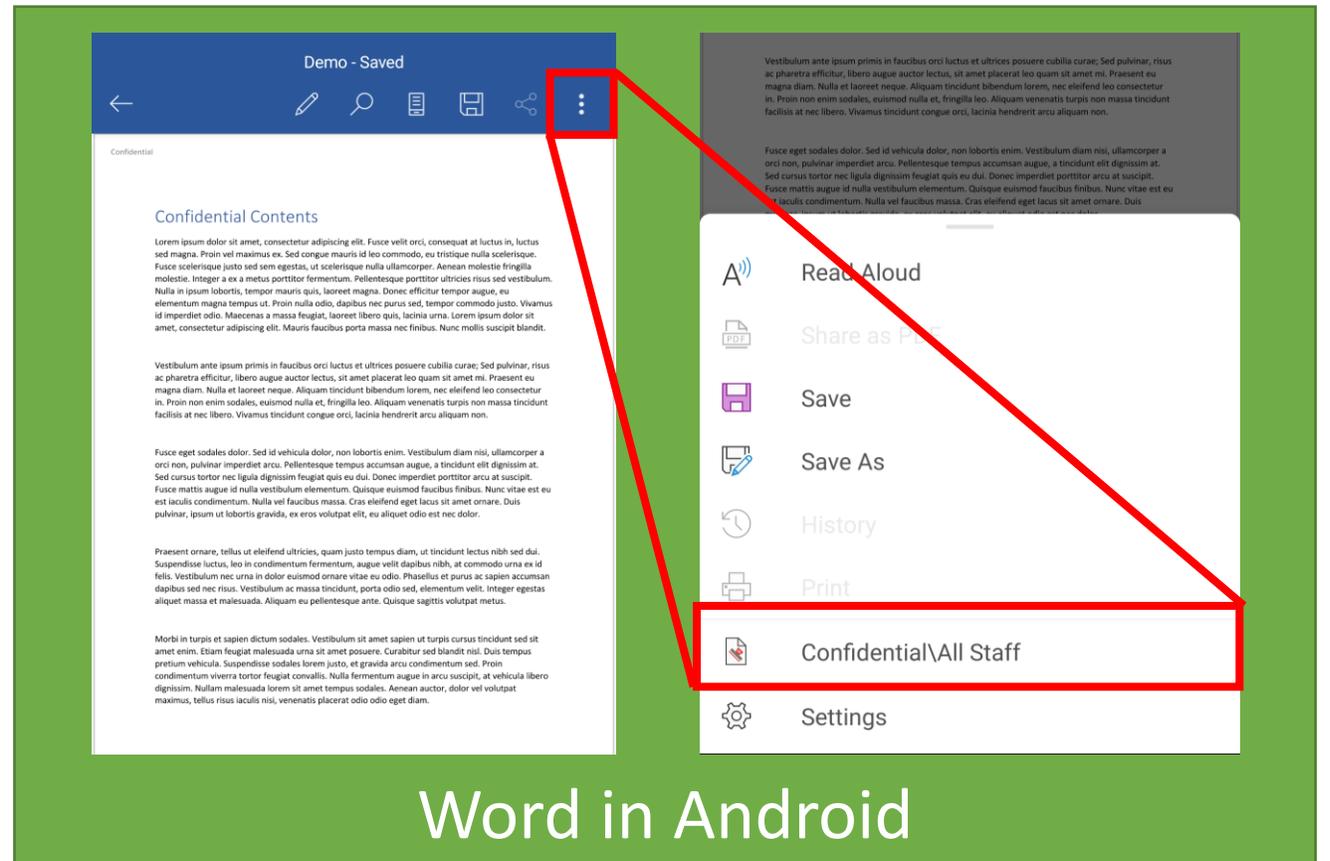
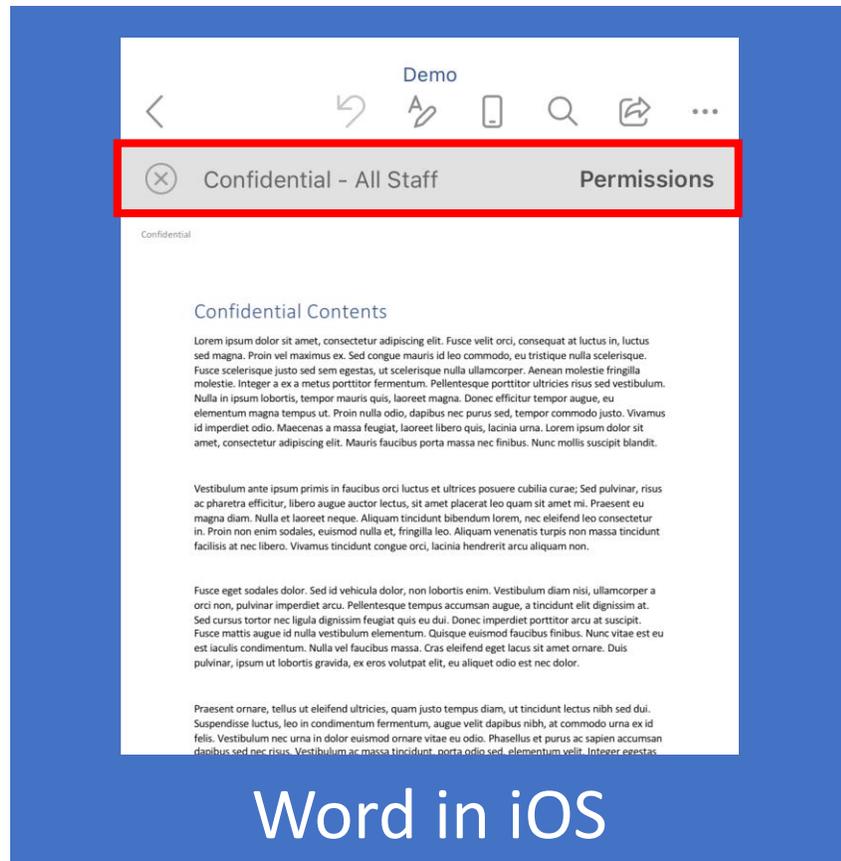
- Corresponds to [Data Classification and Data Governance Policy](#).

Classification Label	Permissions to <u>all Staff</u>		Visual Markings in Office Documents* / Emails	Offline Access
Strictly Confidential – All Staff	<ul style="list-style-type: none"> ✓ View ✓ Reply / Reply-all 	<ul style="list-style-type: none"> × Edit × Save / Save-as / Export × Print × Forward × Copy-n-paste / screenshot 	<p>Header, and Footer</p> <p>Watermark (for Office Documents only)</p>	1 day
Confidential – All Staff	<ul style="list-style-type: none"> ✓ View ✓ Edit ✓ Save / Save-as / Export ✓ Reply / Reply-all / Forward 		Header and Footer	7 days

* Microsoft Word (.docx), Excel (.xlsx) and PowerPoint (.pptx)

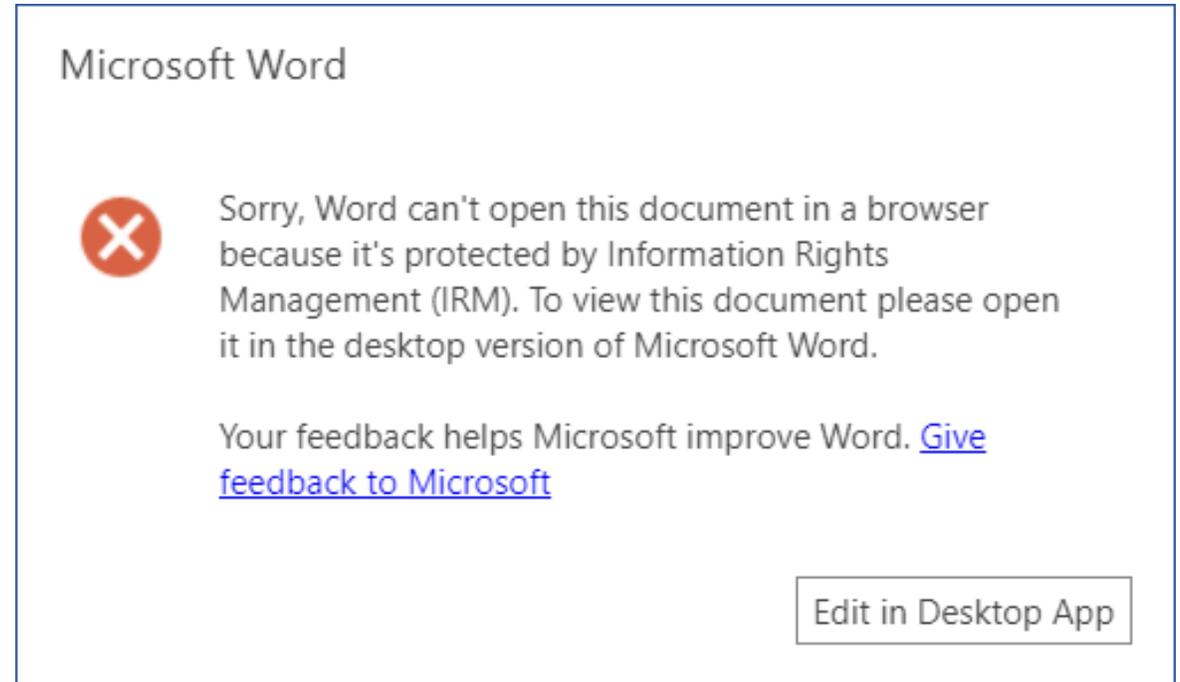
Open Office Documents from Mobile Device

- Use official Microsoft Office apps.



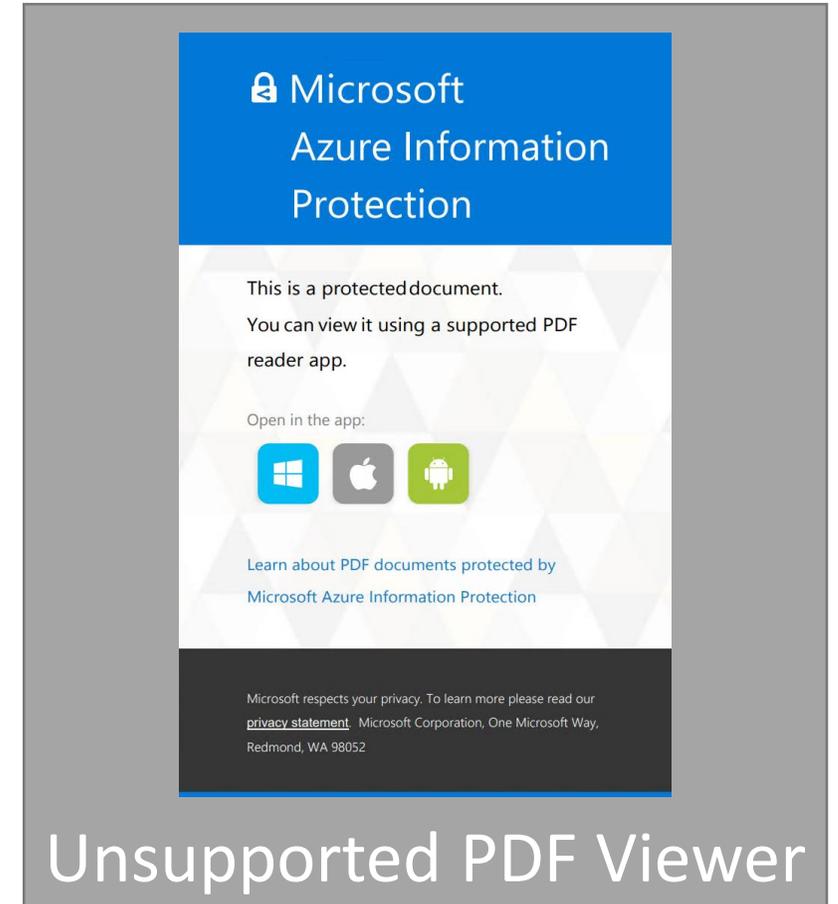
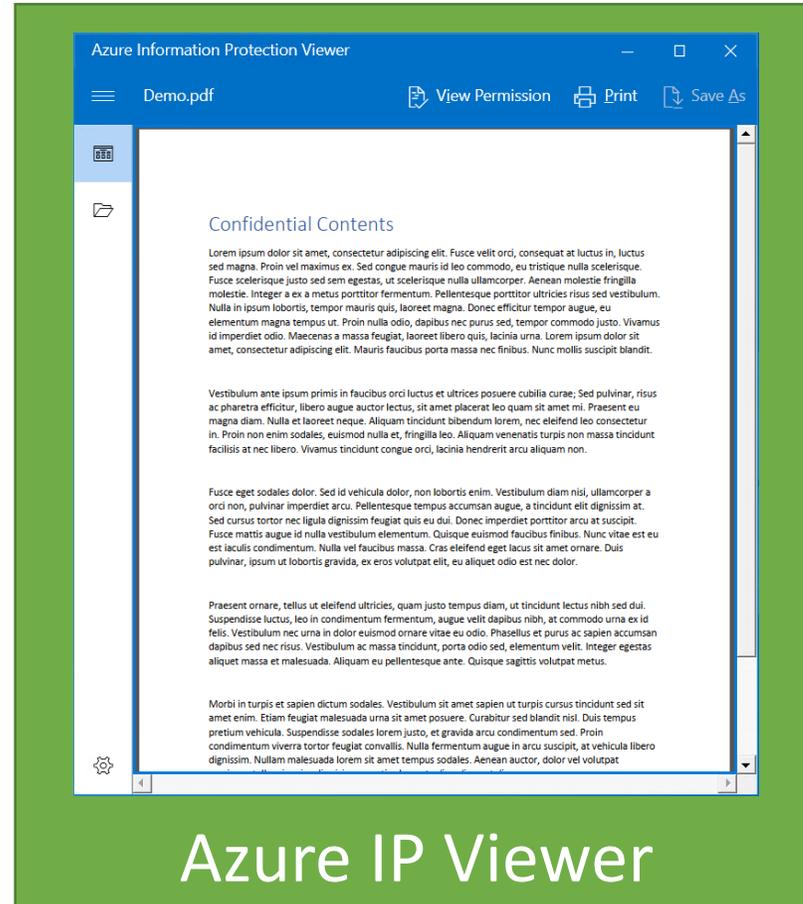
Open Office Documents in Office 365, OneDrive and SharePoint (web)

- Currently **not supported**. Please **open protected files using desktop or mobile device**.
- Same for OneDrive and SharePoint unless files are opened in desktop app via a network drive.

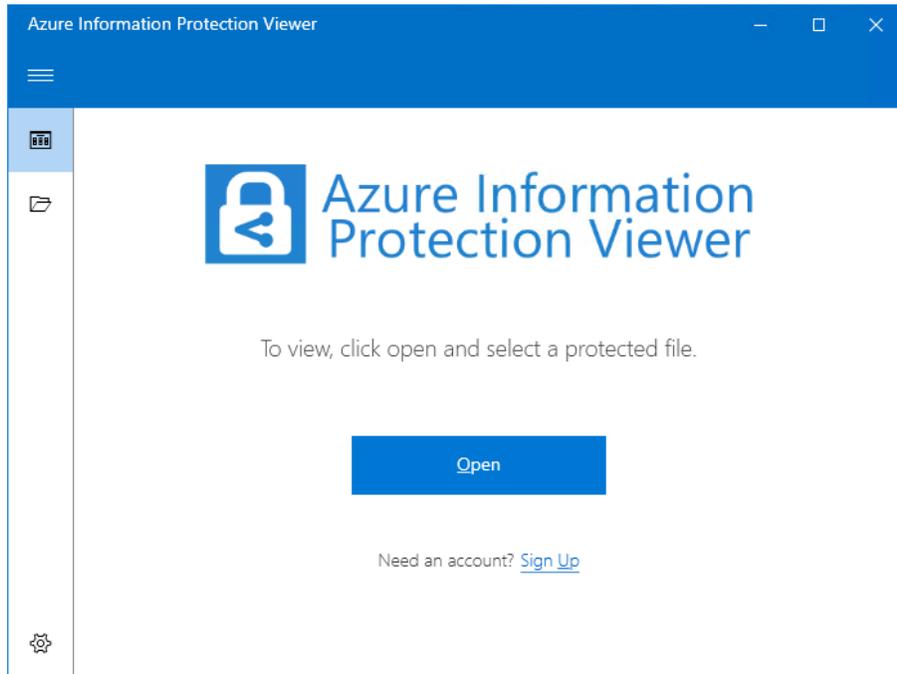


Open PDF Documents

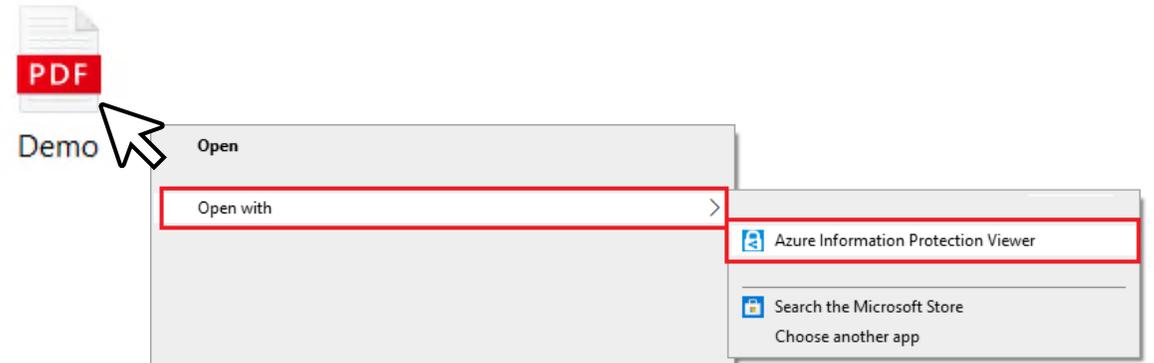
- Use Azure Information Protection Viewer.
- Standard message will be shown for unsupported PDF viewer.



Open PDF Documents using Azure Information Protection Viewer (Windows)



Launch the app from
Start Menu ...



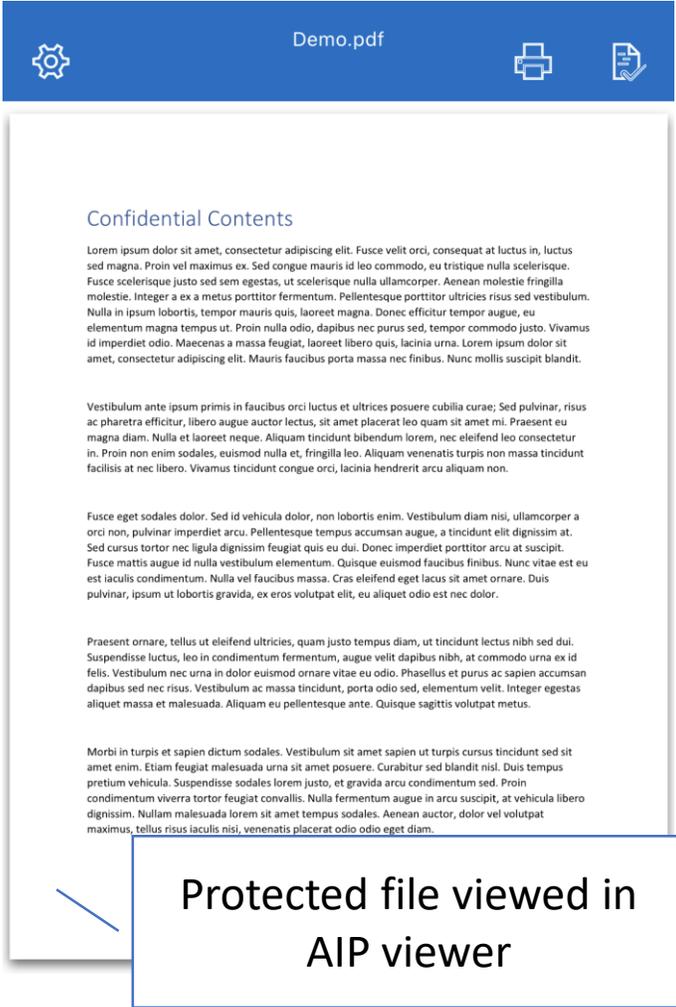
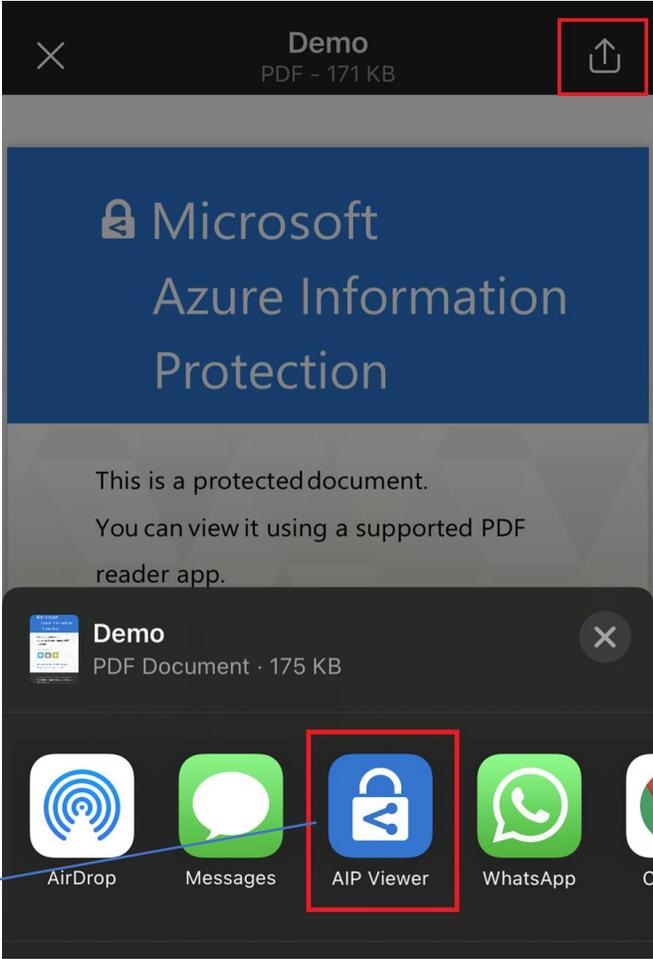
... or right-click the PDF file >
Open with > Azure Information
Protection Viewer

Starting
7 Jan 2021

Open PDF Documents using Azure Information Protection Viewer (iOS / Android)

- Install Azure Information Protection Viewer ([iOS](#) / [Android](#)) prior opening protected PDF files.
- Open protected PDF files in AIP Viewer app.

iOS: 'Share file via...' and pick AIP Viewer

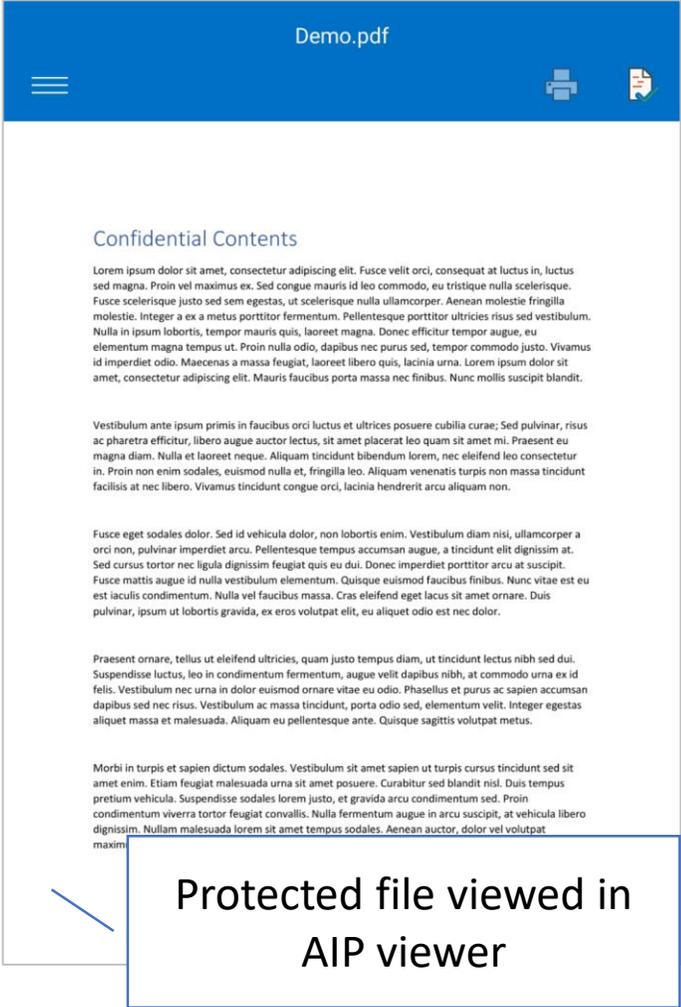
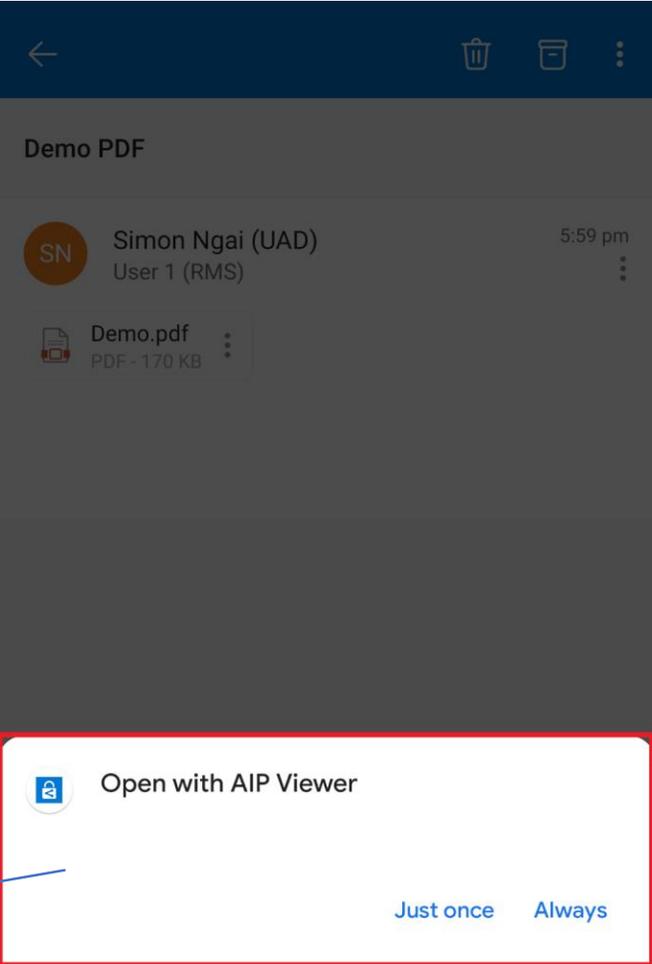


Starting
7 Jan 2021

Open PDF Documents using Azure Information Protection Viewer (iOS / Android)

- Install Azure Information Protection Viewer ([iOS](#) / [Android](#)) prior opening protected PDF files.
- Open protected PDF files in AIP Viewer app.

Android: Choose AIP Viewer when prompted



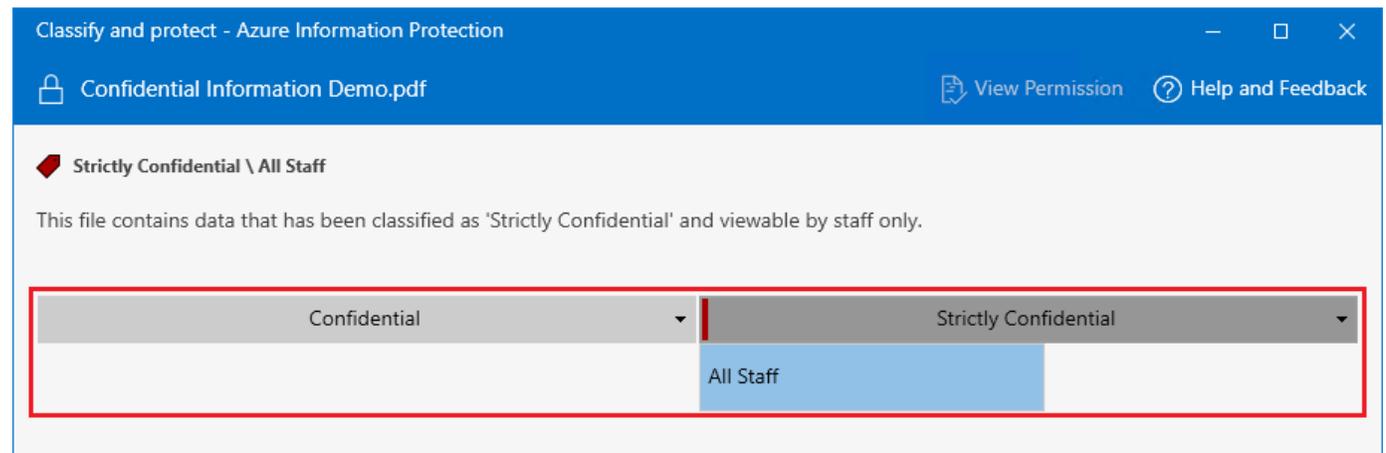
Protected file viewed in AIP viewer

Create Protected PDF Document using Azure Information Protection App (Windows)

1. Right-click the PDF file and click 'Classify and protect' from the context menu.



2. Select preferred protection and click 'Apply' from AIP app.



Send Protected Email

- Protect your email using the same way as protecting your documents.

The screenshot displays the Microsoft Word interface for composing an email. The ribbon includes 'File', 'Message', 'Insert', 'Options', 'Format Text', and 'Review'. The 'Sensitivity' dropdown menu is open, showing options like 'High Importance' and 'Low Importance'. A red box highlights the 'Strictly Confidential \ All Staff' label in the ribbon, and a blue box highlights the 'Strictly Confidential - All Staff' label in the email header. A blue arrow points from the ribbon label to the header label. Another blue box highlights the 'Confidential Contents' watermark in the email body, with a blue arrow pointing from the ribbon label to it.

1. Select the classification label

2. Classification Label applied to the email

Strictly Confidential \ All Staff

Confidential

Strictly Confidential

Strictly Confidential - All Staff - This file contains data that has been classified as 'Strictly Confidential' and viewable by staff only.
Permission granted by: demouser@cuhk.edu.hk

To... User 1 (RMS);

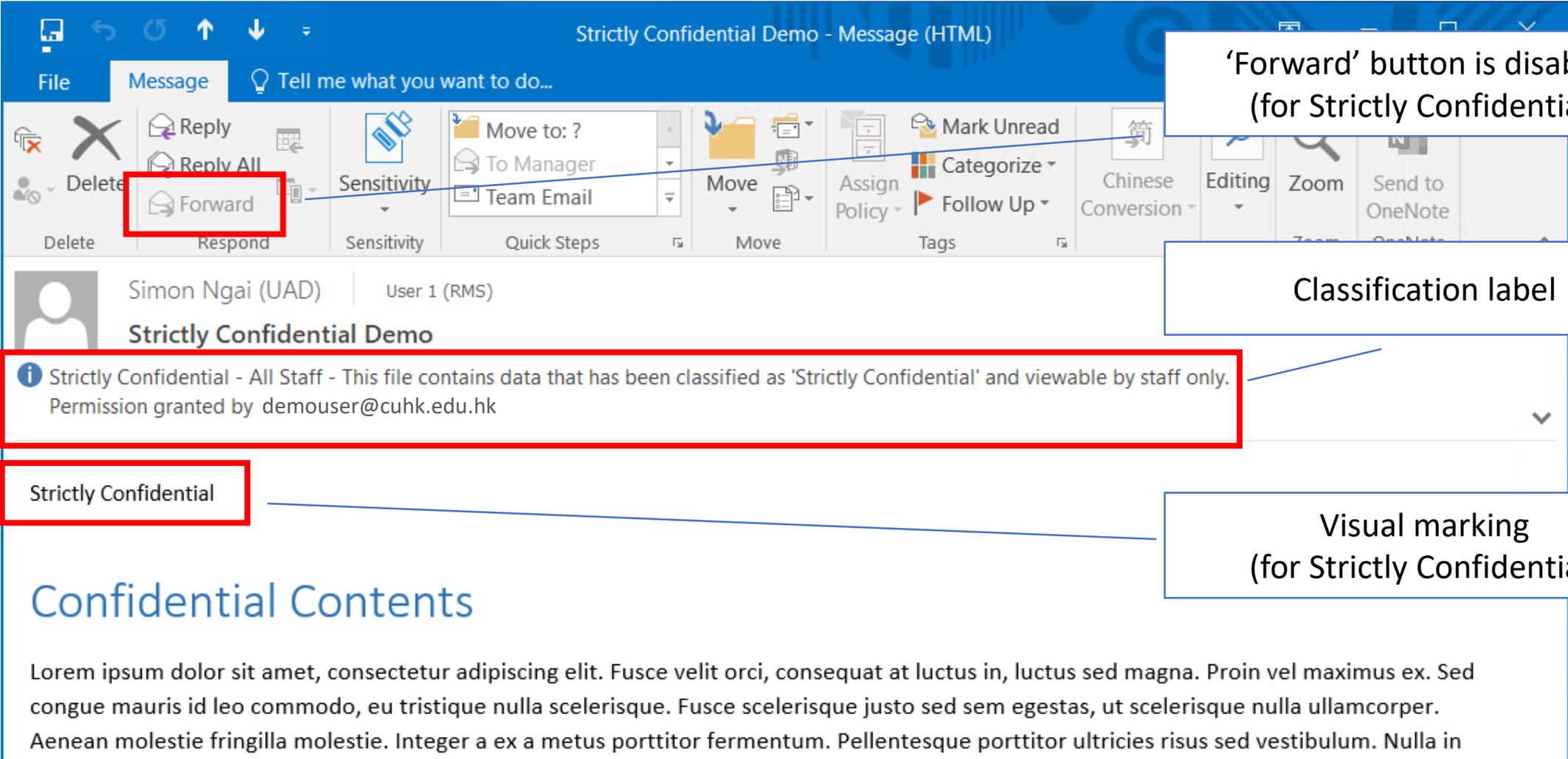
Cc...

Subject Protected Email Demo

Confidential Contents

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce velit orci, consequat at luctus in, luctus sed magna. Proin vel maximus

Read Protected Email (by CUHK Staff)



'Forward' button is disabled (for Strictly Confidential)

Classification label

Strictly Confidential

Visual marking (for Strictly Confidential)

Send Protected Email (Tips)

- Put #confidential and #strictlyconfidential hashtag in your email subject to achieve the same result

Subject includes appropriate hashtag

The screenshot shows the Microsoft Word ribbon with the 'Message' tab selected. The ribbon includes sections for 'Attachments', 'Quick Steps', 'Move', 'Tags', 'Chinese Conversion', 'Editing', and 'Zoom'. The 'Sensitivity' section is highlighted, showing a dropdown menu with options: 'Move to: ?', 'To Manager', and 'Team Email'. The 'Sensitivity' dropdown is set to 'Strictly Confidential'. The ribbon also shows 'Delete', 'Respond', 'Sensitivity', 'Quick Steps', 'Move', 'Tags', 'Chinese Conversion', 'Editing', and 'Zoom' groups.

Simon Ngai (UAD) | User 1 (RMS); User 2 (RMS); User 3 (RMS) ▾
Email with unprotected word attachment Subject tag #strictlyconfidential

**Strictly Confidential - All Staff - This file contains data that has been classified as 'Strictly Confidential' and viewable by staff only.
Permission granted by: demouser@cuhk.edu.hk**

Classic 2019 Unprotected.docx
744 KB

Confidential Contents

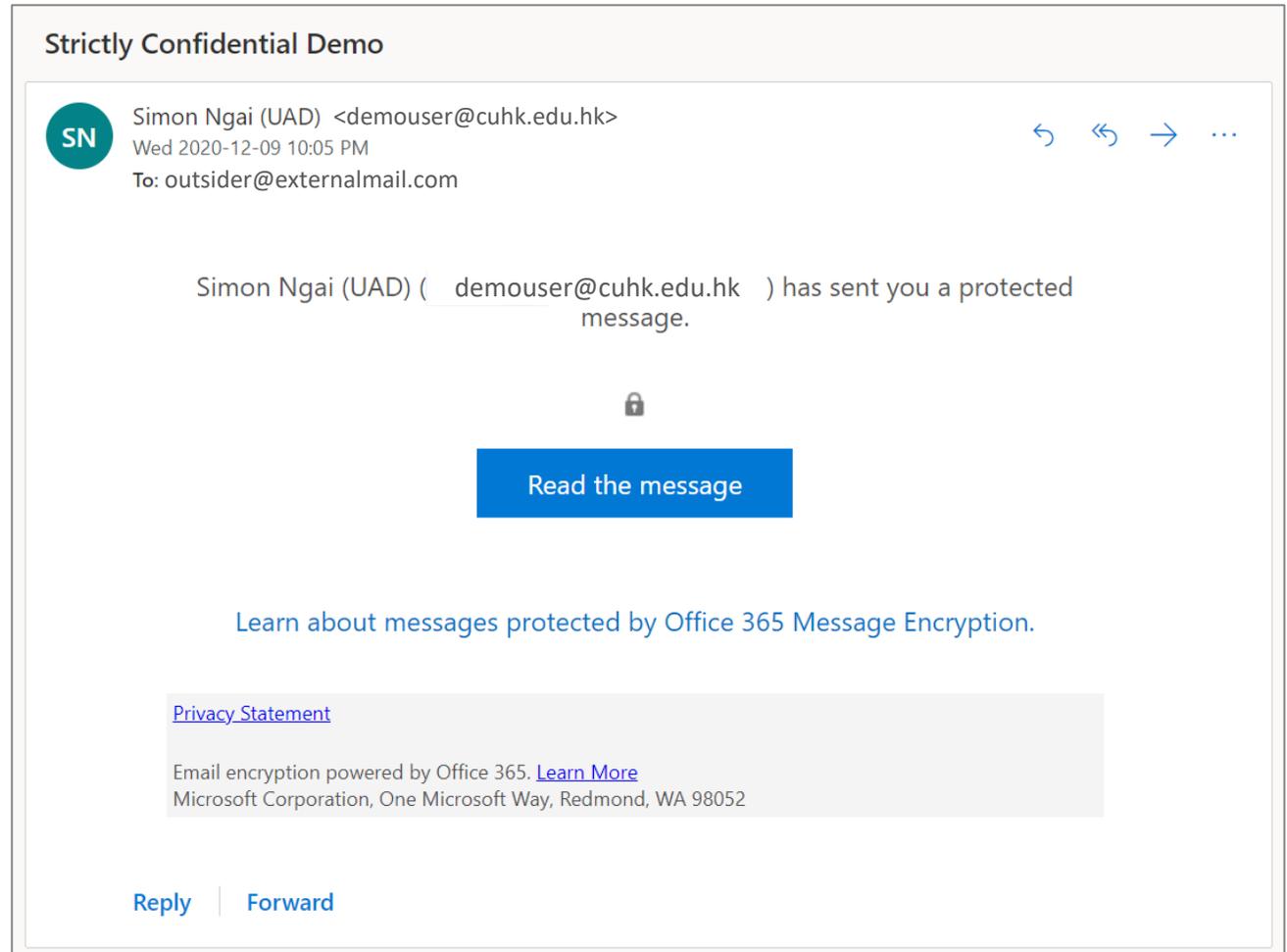
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce velit orci, consequat at luctus in, luctus sed magna. Proin vel maximus

Classification label applied

Attachment and content will have corresponding restrictions applied, through visual marking is not available

Read Protected Email (by Outsider)

- In case sender send out the email to a non-CUHK email address, outsider won't have access to the protected email.



Start Protect
Your Documents
TODAY!

A stylized illustration of a laptop computer. The screen displays a document with a header and several lines of text. A light blue shield with a white outline is positioned over the document, symbolizing protection. The laptop is shown in a light brown color.

Demo

Create Protected Documents

- Word
- PDF

View Protected Documents

- By CUHK Staff
- By Outsiders

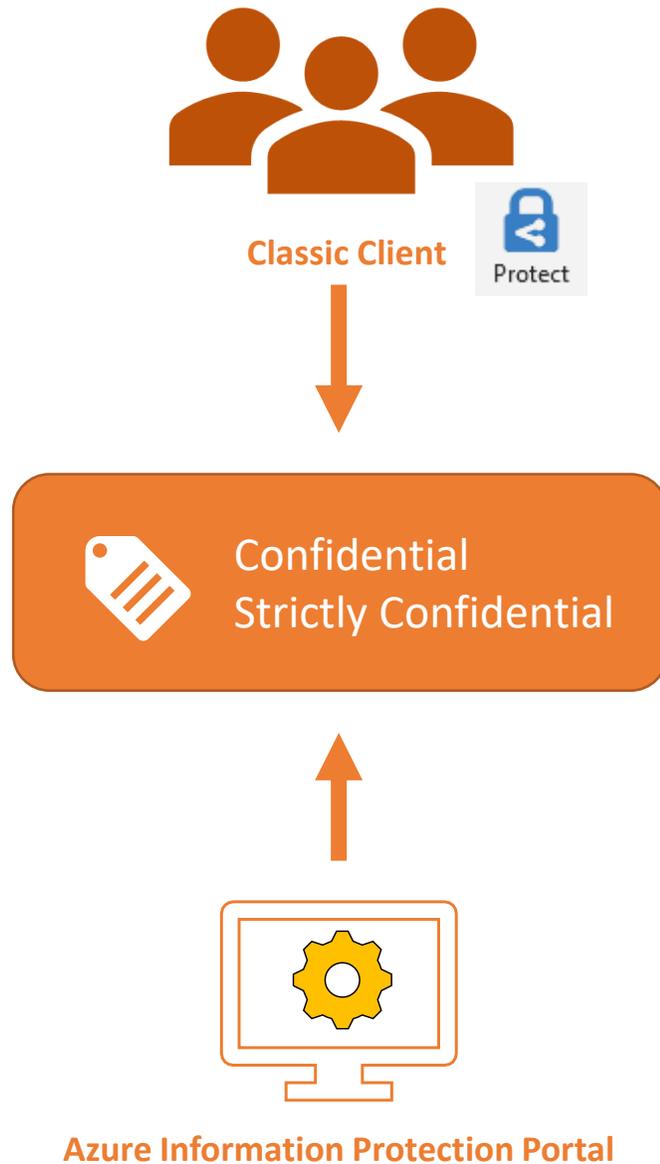
Send Protected Email

View Protected Email

- By CUHK Staff
- By Outsiders



Migrate from
Classic Client to
Unified Labeling
Client



Classic Client (v1)

Based on Azure Information Protection

- ✓ Word / Excel / PowerPoint Desktop
- ✓ Outlook Desktop
- × Word / Excel / PowerPoint Mobile
(Requires AIP viewer)
- × Outlook on the web
- × Acrobat Reader

Source: [Announcing timelines for sunseting label management in the Azure portal and AIP client \(classic\) - Microsoft Tech Community](#)

Source: [Understanding Unified Labeling migration - Microsoft Tech Community](#)

Unified Labeling Client (v2)

Based on Microsoft 365 Security and Compliance Center

- ✓ Word / Excel / PowerPoint Desktop
- ✓ Outlook Desktop
- ✓ Word / Excel / PowerPoint Mobile
- ✓ Outlook Mobile
- ✓ Office for the web (coming soon)
- ✓ Outlook for the web
- ✓ Power BI Data protection
- ✓ Apps based on Microsoft Information Protection SDK (e.g. Adobe Acrobat)

Source: [Announcing timelines for sunseting label management in the Azure portal and AIP client \(classic\) - Microsoft Tech Community](#)

Source: [Understanding Unified Labeling migration - Microsoft Tech Community](#)





Azure Portal

Label Management in Azure Portal will no longer be available after 31 Mar 2021



Classic Client

Protect

Classic client will no longer work after 31 Mar 2021



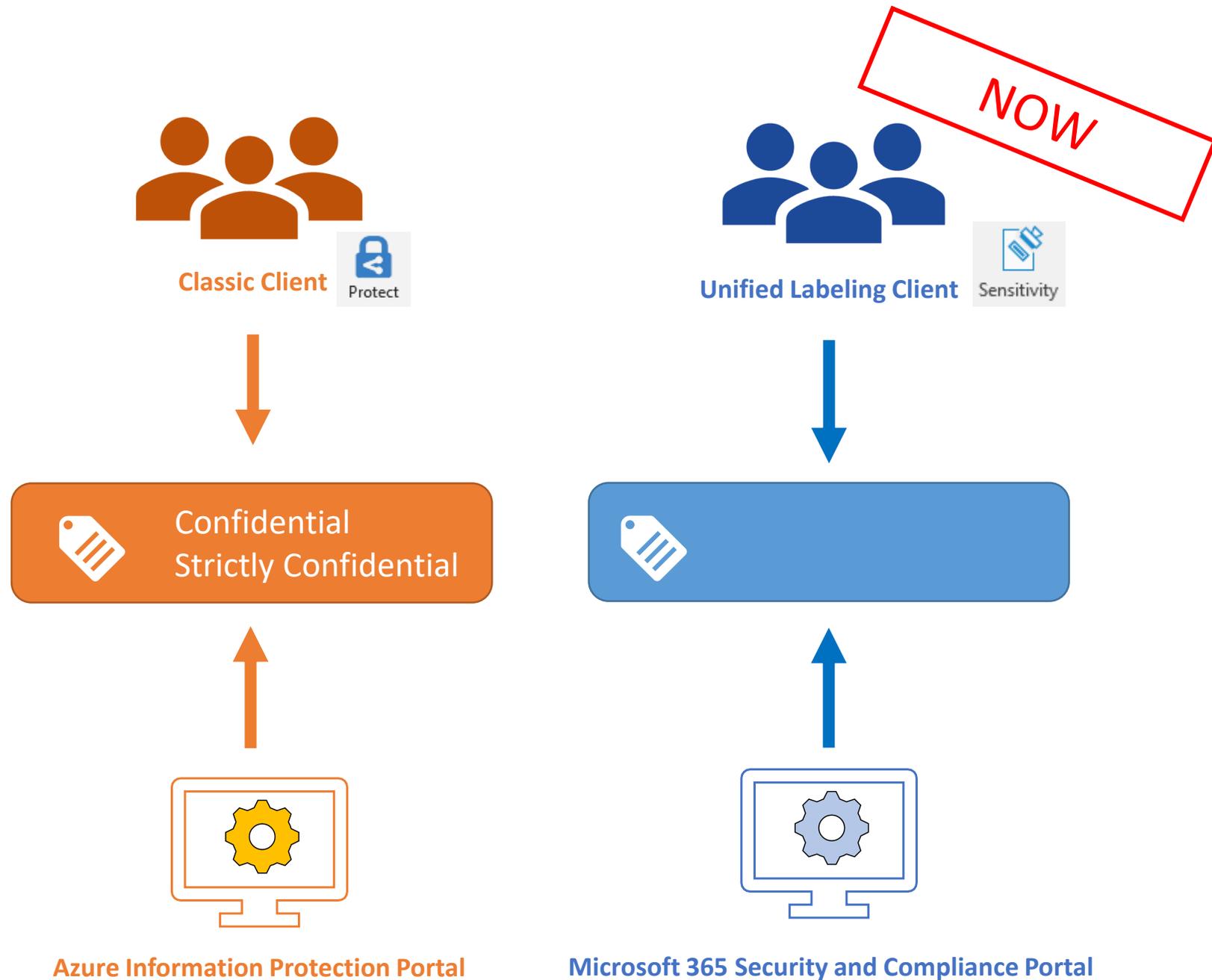
Migration Anatomy



Stage 1

(Now – 6 Jan 2021)

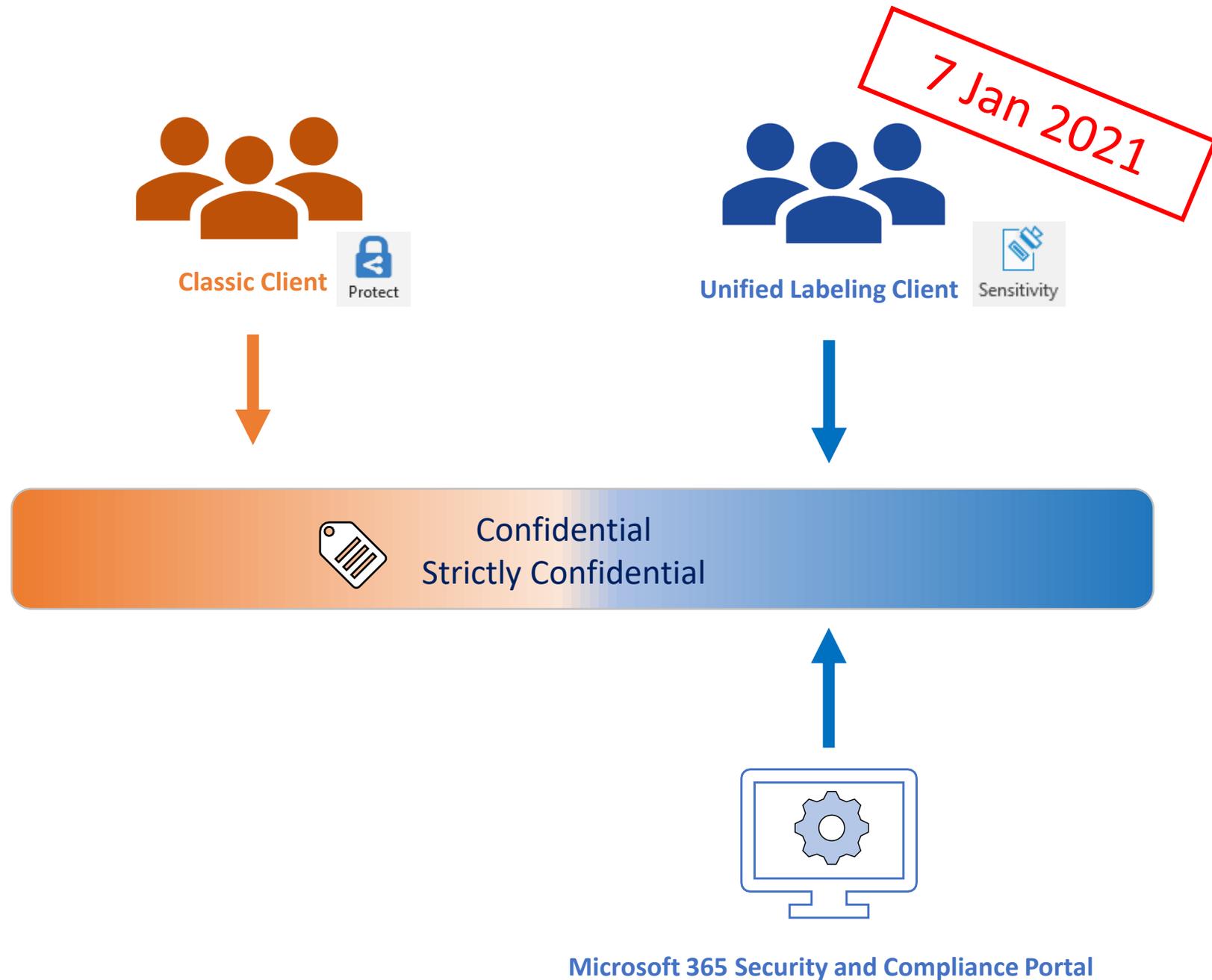
- Preparation work by ITSC.
- You: No action needed – apply document protection as usual.



Stage 2

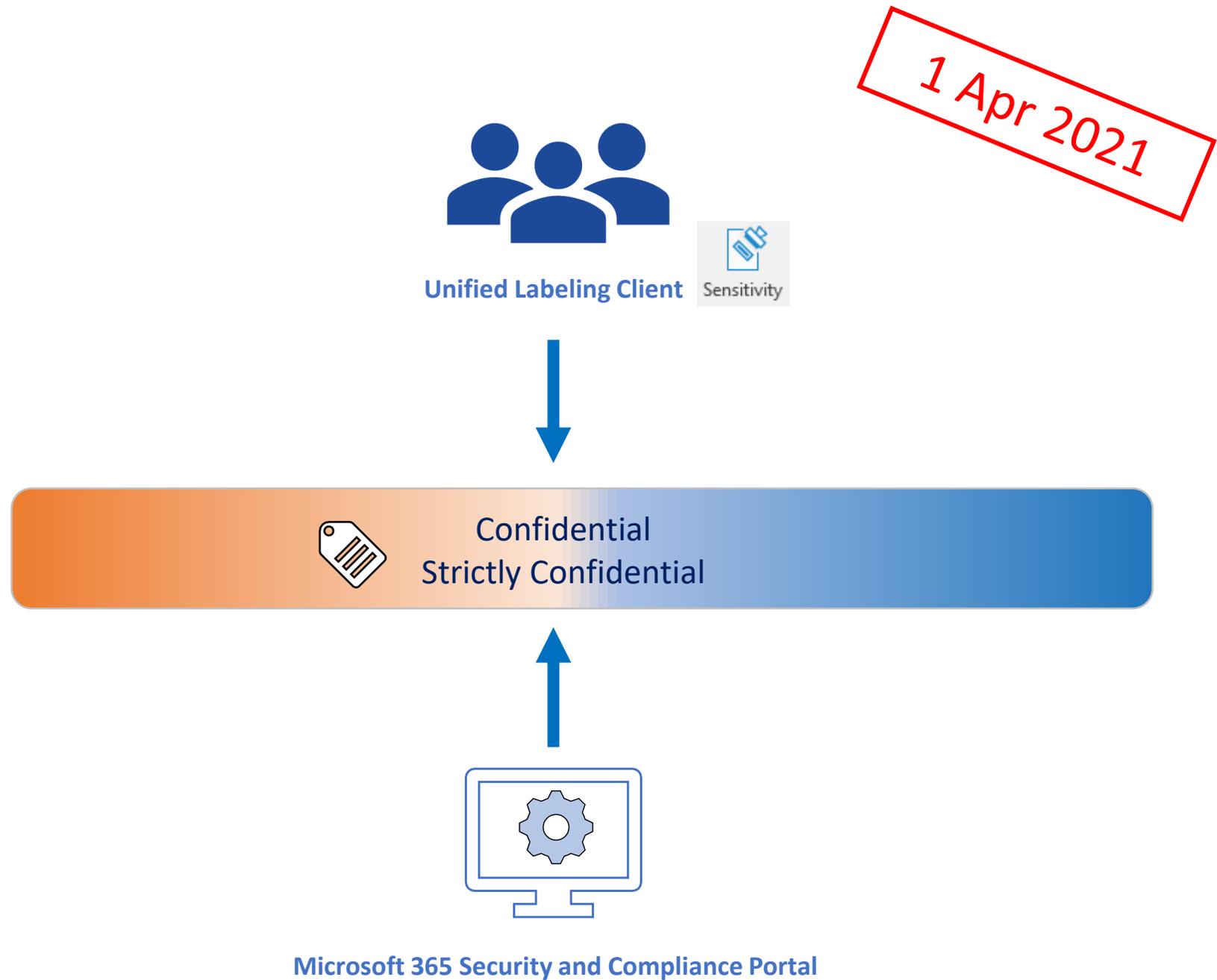
(7 Jan – 31 Mar 2021)

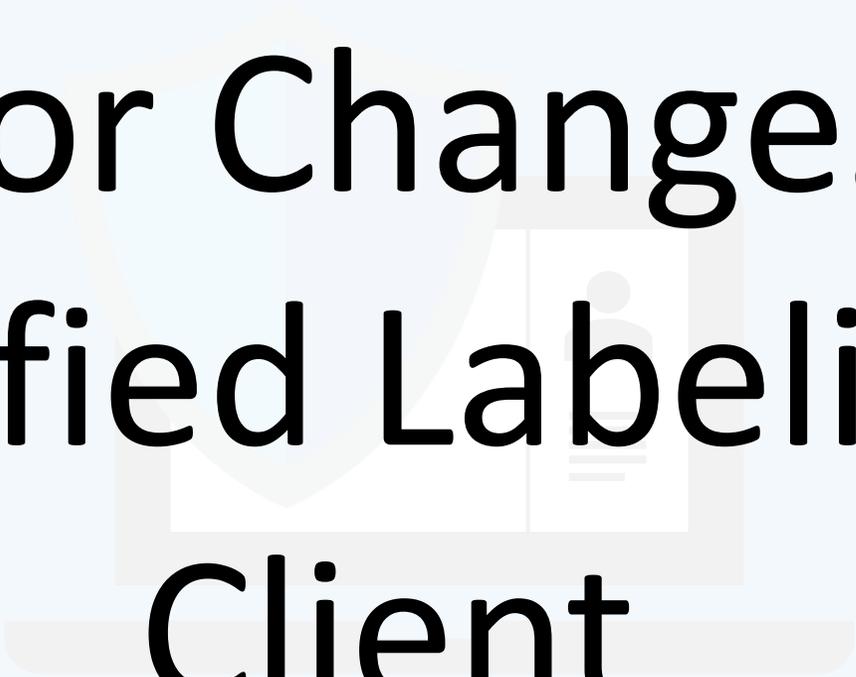
- Transition period. User should upgrade to Unified Labeling client.
- Protected documents created by either client can be opened by the other.



Stage 3
(1 Apr 2021 onwards)

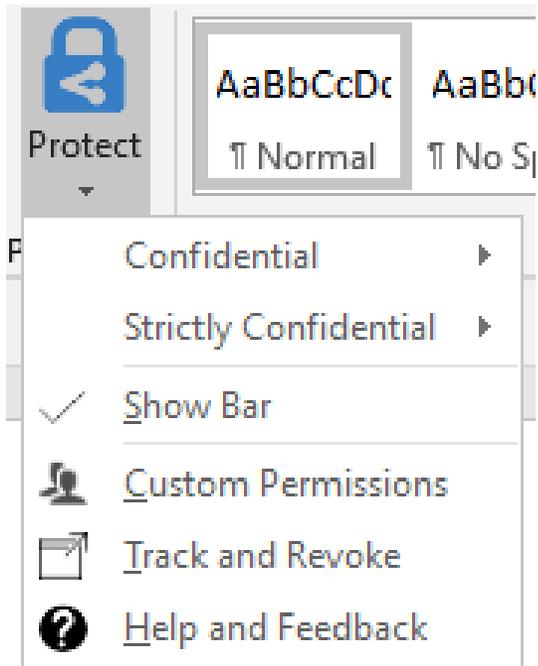
- Users are expected to read and create protected contents using Unified Labeling (i.e. new) client.
- Files protected using Classic client can still be opened.



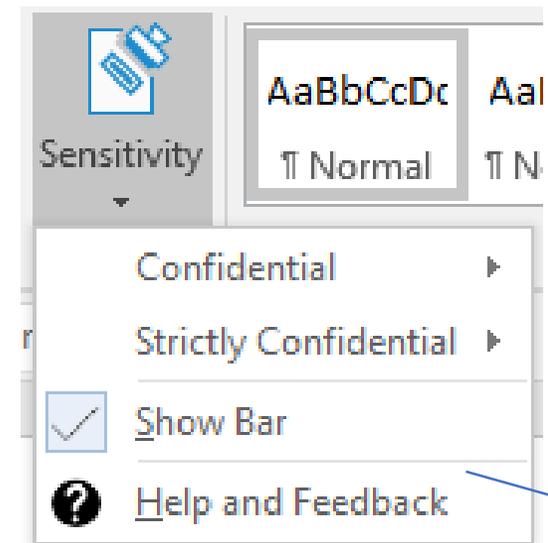


Major Changes in Unified Labeling Client

Major Changes in Unified Labeling Client



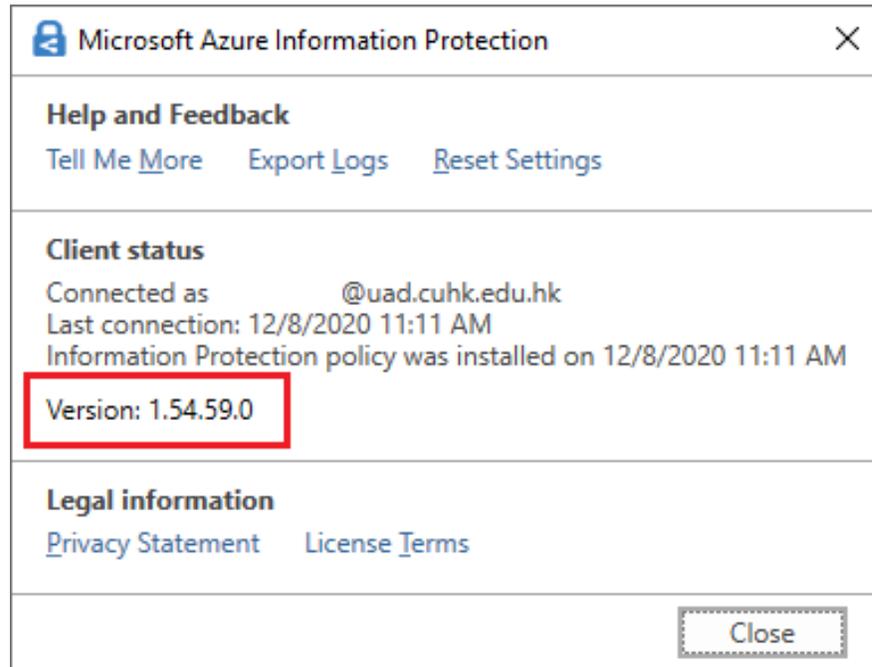
Classic Client



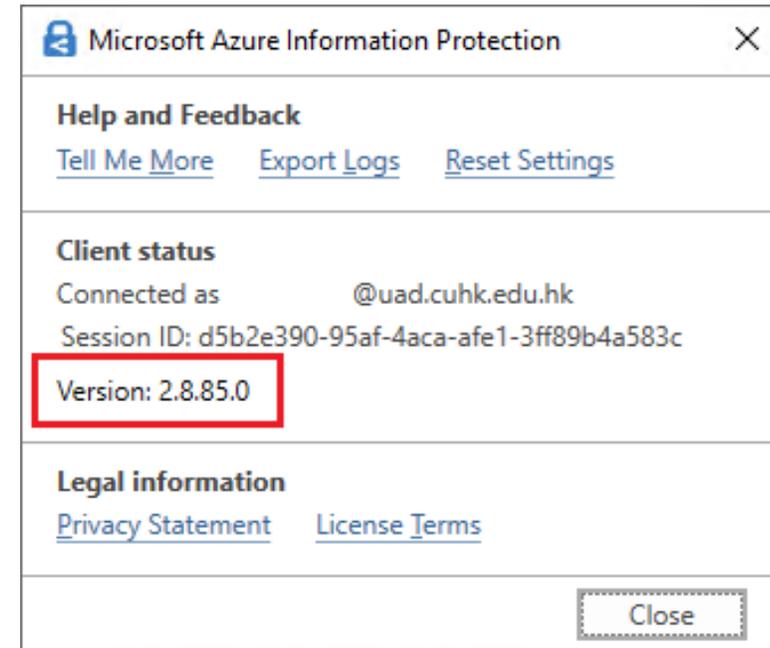
'Custom Permissions' no longer accessible from Office app
'Track and Revoke' is no longer supported

Unified Labeling Client

Major Changes in Unified Labeling Client



Classic Client

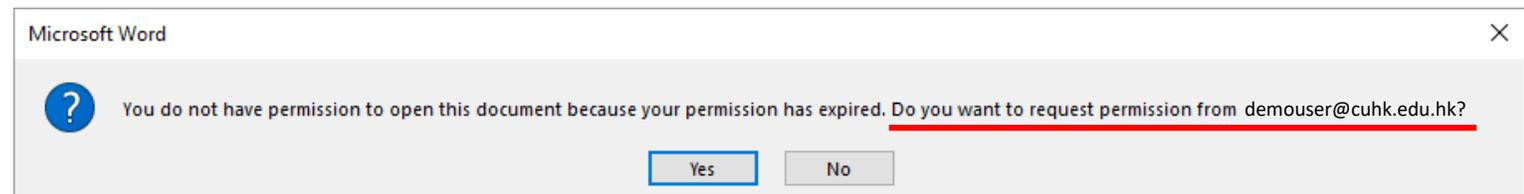


Unified Labeling Client

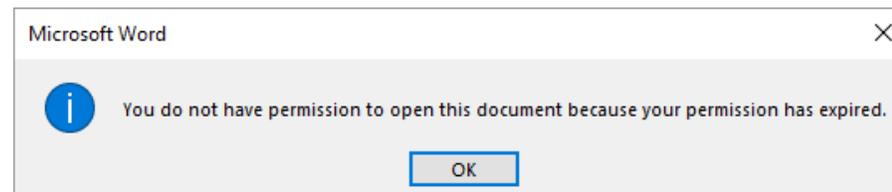
Major Changes in Unified Labeling Client

Feature	Description
Creation of protected PDF files using .ppdf extension	<ul style="list-style-type: none">• PDF files are protected using ISO standard (i.e. using .pdf extension)• Still be able to read .ppdf files
Display of the user identity that applied the protection	<ul style="list-style-type: none">• Not planned in Unified Labeling client

Classic



Unified



Installing Unified Labeling Client

itsc Information Technology Services Centre

DATA CLASSIFICATION AND INFORMATION PROTECTION

HOME >> ALL >> INFORMATION SECURITY >> DATA CLASSIFICATION AND PROTECTION WITH AZURE INFORMATION PROTECTION

Data Classification and Protection with Azure Information Protection (AIP)

To cope with the Data Classification and Data Governance Policy for protecting University's digital information, an information protection system with **Azure Information Protection - AIP**, (formerly Right Management Service - RMS), is implemented for protecting digital information according to the defined data class.

Available to
Departments

Service Charge and Application
Free; no application required

Service Availability
Office hours

General Enquiry or Azure information Protection (AIP)

3. User Manuals and Briefing Sessions

4. Installation Files

For standalone installation, please download and extract the installation file "AZInfoProtection.exe". (For Windows only)

For central deployment, please download and extract the MSI file "AZInfoProtection_MSI_for_central_deployment.msi" instead.

5. FAQ

Major Projects | IT Policies | Application Forms | User G

香港中文大學
The Chinese University of Hong Kong

Details will be announced by
7 Jan 2021

'AzInfoProtection_UL.exe' for
general users

'AzInfoProtection_UL_MSI_for_central_dep
loyment.msi' for mass deployment

[ITSC Website > Services > Information Security >
Data Classification and Protection with Azure Information Protection \(AIP\)](#)

Migration Timeline Recap

7 January – 31 March 2021

- Users who need to create / frequently access protected documents should upgrade their IP client starting 7 Jan 2021.

From 1 April 2021

- Users must use Unified Labeling (new) client to create and open protected documents.
- Documents created by Classic Client could still be opened by Unified Labeling client.
- All AIP (old) clients should be removed.

Questions?



Frequently Asked Questions

1. Can a protected document be created using a Project Account ?
 - AIP service is also enabled for project accounts.
 - When a protected document is sent to project account (via email), users can open the protected document using his / her user identity.

Frequently Asked Questions

2. My faculty member used to forward all University emails to his/her personal email (e.g., Gmail). Does AIP also work in this scenario?
 - Protected email does NOT work (requires @cuhk.edu.hk mailbox).
 - Protected attachment that included in an unprotected email works. Please be reminded that to view the protected document, users are required to either (1) install latest AIP viewer or, (2) from 7 Jan 2021 onwards, open the protected file using Office 2019/Office365.

Starting
7 Jan 2021

Frequently Asked Questions

3. Can I send a message to student / alumni / vendor and don't allow them to forward it?

- This is an advanced topic, achievable using Outlook on the web only and available on or after 7 Jan 2021.
- **CAUTION:** do not mix up with 'labels' which is targeted to CUHK staff

Label / Custom Security Level	Target	Read	Copy	Forward	Open by Outsider
Label: Strictly Confidential – All Staff	CUHK Staff (@cuhk.edu.hk)	Yes	No	No	No
Label: Confidential – All Staff	CUHK Staff (@cuhk.edu.hk)	Yes	Yes	Yes	No
Encrypt	Specific recipient	Yes	Yes	Yes	Yes (using OTP*)
Do Not Forward	Specific recipient	Yes	No	No	Yes (using OTP*)

* One-time passcode

Starting
7 Jan 2021

Frequently Asked Questions

3. (Continued)

- Compose a message in Outlook on the web. Click ellipsis (...) button > Encrypt > Do Not Forward.

The screenshot shows the Outlook on the web interface. The top navigation bar includes the Outlook logo, a search bar, and a 'New message' button. The main toolbar contains 'Send', 'Attach', 'Sensitivity', and 'Discard' buttons. An ellipsis (...) button is highlighted with a red box. A context menu is open over this button, listing various actions. The 'Encrypt' option is highlighted with a red box, and its sub-menu is open, showing 'Do Not Forward' as the selected option, also highlighted with a red box. A yellow callout box points to the ellipsis button with the text: 'DON'T choose 'Sensitivity' as it doesn't apply to outsiders.'

Outlook

Search

New message

Send Attach Sensitivity Discard ...

Do Not Forward: Recipients can't forward, print, or copy content

To outsider@gmail.com

Cc

Message to outsider - DO NOT FORWARD

Please do not forward this message.

Save draft

Insert signature

Show From

Encrypt > Encrypt

Set importance > ✓ Do Not Forward

Show message options...

Switch to plain text

Check for accessibility issues

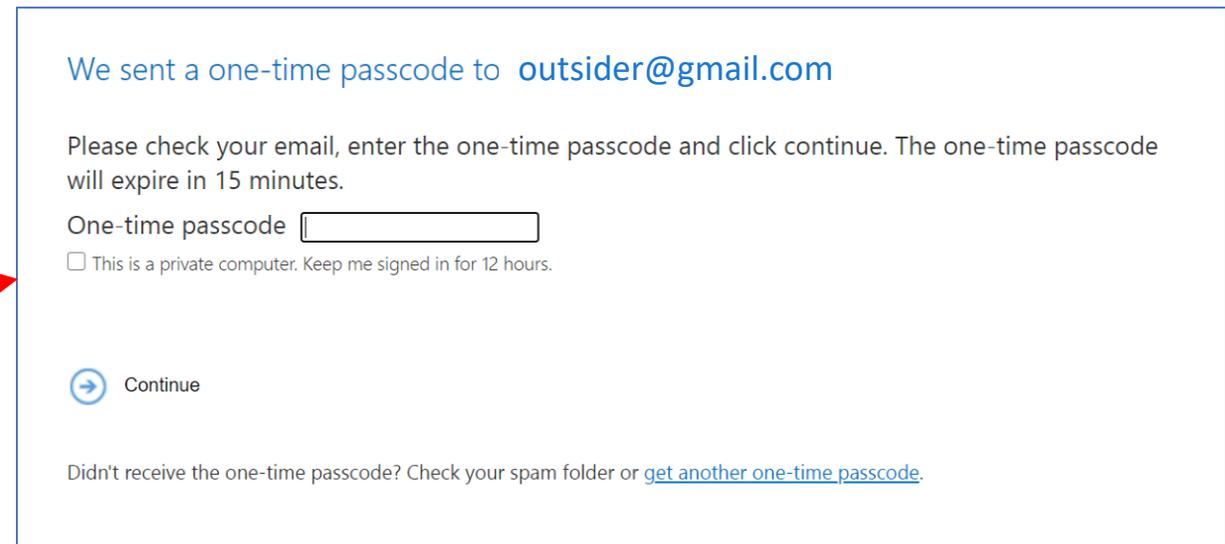
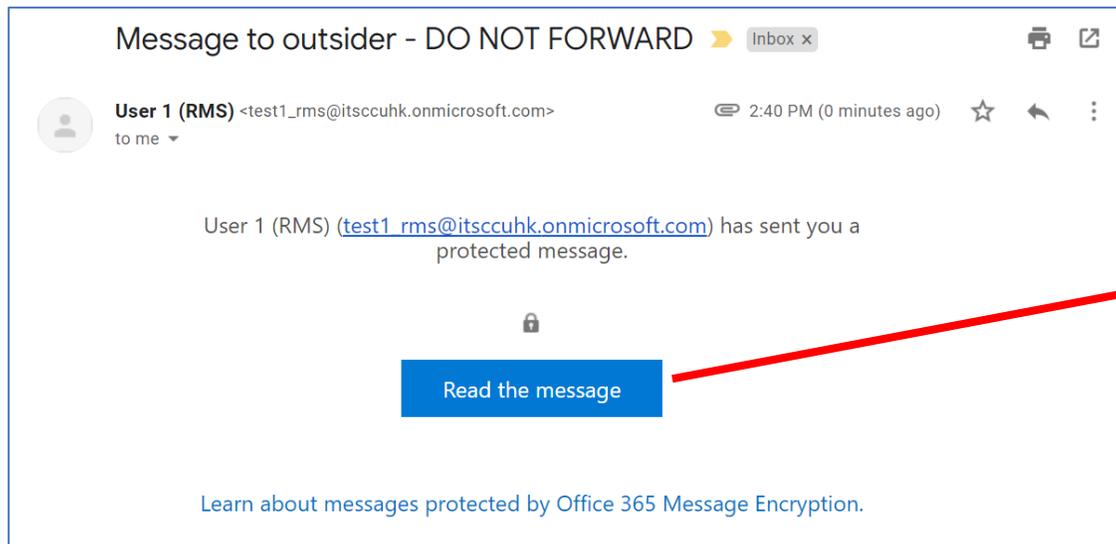
DON'T choose 'Sensitivity' as it doesn't apply to outsiders.

Starting
7 Jan 2021

Frequently Asked Questions

3. (Continued)

- Recipient will be asked to enter a one-time passcode. The code will be sent to user's mailbox as soon as 'Read the message button' is clicked.



Starting
7 Jan 2021

Frequently Asked Questions

3. (Continued)

- Outsiders will see the message upon successful validation. Note Forward and Print buttons are disabled.

The screenshot shows an email interface for the user 'outsider@gmail.com'. The message is titled 'Message to outsider - DO NOT FORWARD'. The sender is 'User 1 (RMS) <test1_rms@itsccuhk.onmicrosoft.com>' with a timestamp of 'Today, 2:40 PM'. A grey banner across the message reads 'Do Not Forward: Recipients can't forward, print, or copy content.' Below this, the text says 'Please do not forward this message.' A context menu is open over the message, showing options: 'Reply', 'Reply all', 'Forward', and 'Print'. The 'Forward' and 'Print' options are greyed out, indicating they are disabled. Two callout boxes are present: one pointing to the 'Do Not Forward' banner with the text 'Unable to copy message', and another pointing to the disabled 'Forward' and 'Print' options with the text 'Forward and Print buttons are disabled'.

outsider@gmail.com Sign Out ?

Message to outsider - DO NOT FORWARD

U1 User 1 (RMS) <test1_rms@itsccuhk.onmicrosoft.com>
Today, 2:40 PM
outsider@gmail.com

Do Not Forward: Recipients can't forward, print, or copy content.

Please do not forward this message.

Reply all | v

Reply
Reply all
Forward
Print

Unable to copy message

Forward and Print buttons are disabled

Appendix 1: Possible User Scenario (since 7 January 2021)

	Scenario	Changes / Impact
1	Office 2016 AIP classic client NOT installed	No Change
2	Office 2016 AIP classic client installed	No Change
3	Office 2019 / Office 365 AIP classic client NOT installed	No Change if user don't sign in Office. After signed in Office 365, <ul style="list-style-type: none"> • "Sensitivity" button will be shown • No more "Track and Revoke" function • The function "Custom Permission" will disappear under "Sensitivity" button.
4	Office 2019 / Office 365 AIP classic client installed	No Change
5	OWA Email Encryption	<ul style="list-style-type: none"> • The change applies to ALL users, NOT depending on AIP client version. • All the 2 labels are available under the "Sensitivity" button. • "Encrypt" and "Do Not Forward" is moved under "... > Encrypt"

Appendix 2: Summary of Changes in Office Add-in and AIP Bar

(A): Stage 1 / (B) : Stage 2

AIP = Class (old) client / MIP = Unified Labeling (new) client

	Conditions	“Protect” button (Related to AIP client)	“Sensitivity” button (No Track and Revoke function) (Related to Unified Labeling)	AIP Bar (Related to AIP classic client or AIP unified client)
1	Office 2016, NO AIP client	(A) No (B) No	(A) No (B) No	(A) No (B) No
2	Office 2016, installed AIP classic client	(A) Yes (B) Yes	(A) No (B) No	(A) Yes (B) Yes
3	Office 2016, installed MIP unified labeling client	(A) No (B) No	(A) Yes (Sign in O365 but return Error Message: "Something went wrong while downloading your template.") (B) Yes (Sign in O365 during client installation)	(A) No (B) No (default) Yes (User need to click "Sensitivity" > "Show Bar" to make it visible.)
4	Office 2019 and Office 365, NO AIP/MIP client	(A) No (B) No	(A) No (B) No (default) / Yes (After sign in O365)	(A) No (B) No
5	Office 2019 and Office 365, installed AIP classic client	(A) Yes (B) Yes	(A) No (B) No	(A) Yes (B) Yes
6	Office 2019 and Office 365, installed MIP unified labeling client	(A) No (B) No	(A) Yes (Sign in O365 but return Error Message: "Something went wrong while downloading your template.") (B) Yes (Sign in O365 during client installation)	(A) No (B) No (default) Yes (User need to click "Sensitivity" > "Show Bar" to make it visible.)
7	OWA Email Encryption		(A) “Encrypt” button (B) All the 2 labels are available under the "Sensitivity" button. Also, "Encrypt" and "Do Not Forward" is moved under "... > Encrypt“	