#### Azure AIP Portal Label & Policy Management Admin Experience - Post March 31st Deprecation

To provide a unified and streamlined customer experience, the Azure Information Protection labeling and policy management in the Azure Portal, and the AIP classic client, will be deprecated on March 31<sup>st</sup>, 2021 as announced in our <u>previous blog</u>.

We highly recommend customers on classic AIP labeling to migrate to unified labeling before this sunset timeline for a seamless transition to unified labeling.

Note: This deprecation does not apply in the following scenarios:

- For customers who have already been approved for extended support. Customers with extended support will continue using the AIP area in the Azure Portal with no impact until the end date of their extended support.
- For GCC/GCC-H/DoD customers. Support is extended for GCC/GCC-H/DoD customers until the end of September 2021.

The deprecation does not affect the Azure Information Protection areas in the Azure portal related to the onpremises scanner and analytics. AIP analytics is still available in the Azure Portal, but we encourage customers to start using the Microsoft 365 Compliance center Activity Explorer.

After deprecation, editing AIP labels and policies in the Azure portal will no longer be available. The only admin action that will still be available after deprecation is to activate unified labeling. Classic client will continue to function as configured; however, no further support is provided, and **maintenance versions will no longer be released for the classic client**.

This blog lists key admin components that will be deprecated and describes how this impacts the admin experience.

For details on migration, see the previous communications on UL migration steps.

#### 1) Admin tries to add new labels in AIP portal

- Admins will not be able to add new labels in the AIP portal.
- The Add a new label link and the ellipses link (...) next to each label will be disabled or removed.
- Admins will not be able to do any of the following:
  - o Add new labels

- Add new sub labels
- o Delete a label
- o Move labels up or down

Fig 1: Home > Azure Information Protection > Labels

Home > Azure Information Protection Azure Information Pro	tection   Labels					×
	≣≣ Columns					
General	A This page is read-only, and current value	s cannot be modified.				
Quick start	Azure Information Protection labeling an configured; however, no further support i To make changes to your labels and label	d policy management in the Azure Portal, is provided, and maintenance versions wi ling policies, you must migrate to unified	as well as the Azure Infi I no longer be released labeling and upgrade to	ormation Protection classic cl for the classic client. the unified labeling client.	ient, reached end-of-life on April 1, 2021. Your current labels and labeling policies will continue to function as	÷
LL Usage report (Preview)						
& Activity logs (Preview)	Label display name	Policy	Marking	Protection		
Data discovery (Preview)	Local	,	~ ~	~		
III Recommendations (Preview)	Public	Local Policy		~		
Classifications	<b>∠</b> 2	Local Policy				
Labels	sub	Local Policy		~		
D Policies						
Scanner						
D1 chater						

# 2) Admin tries to edit labels in AIP portal

- Labels will be set to read-only mode.

Fig 2: Home > Azure Information Protection > Labels > Label Name

Label. Z	
Vicrosoft - Azure Information Protection	
🔜 Save 🗙 Discard 📋 Delete this label	
pecify how this label is displayed in the Information Protection client on user devices	
Off On	
abel display name	
2	
Description	
2	
Color	
Color Select from list Custom	
Color Select from list Custom	$\sim$
Color Select from list Custom Black	$\sim$
Color Select from list Custom Black	v
Color Select from list Custom Black Set permissions for documents and emails containing this label	~
Color Select from list Custom Black Set permissions for documents and emails containing this label	V
Color Select from list Custom Black Set permissions for documents and emails containing this label Not configured Protect Remove Protection	~
Color Select from list Custom Black Set permissions for documents and emails containing this label Not configured Protect Remove Protection Protection	~
Color Select from list Custom Black Set permissions for documents and emails containing this label Not configured Protect Remove Protection Protection Azure (cloud key)	× 
Color Select from list Custom Black Set permissions for documents and emails containing this label Not configured Protect Remove Protection Protection Azure (cloud key)	>
Color Select from list Custom Black Set permissions for documents and emails containing this label Not configured Protect Remove Protection Protection Azure (cloud key)	>
Color Select from list Custom Black Ext permissions for documents and emails containing this label Not configured Protect Remove Protection Protection Azure (cloud key) Ext visual marking (such as header or footer)	>
Color Select from list Custom Black  Set permissions for documents and emails containing this label Not configured Protect Remove Protection  Protection Azure (cloud key)  Set visual marking (such as header or footer) Documents with this label have a header	>
Color Select from list Custom Black Set permissions for documents and emails containing this label Not configured Protect Remove Protection Protection Azure (cloud key) Set visual marking (such as header or footer) Documents with this label have a header Off On	>
Color Select from list Custom Black  Set permissions for documents and emails containing this label  Not configured Protect Remove Protection  Protection Azure (cloud key)  Set visual marking (such as header or footer)  Occuments with this label have a header  Off On  Control on  C	>

- 3) Admin tries to edit label conditions in the AIP portal
- The Add new condition link will be removed.

Fig 3a: Home > Azure Information Protection > Labels > Label Name > Configure Condition

Configure conditions for automatically applying this label $\overset{()}{\smile}$	
If any of these conditions are met, this label is applied	
Condition name	Occurrences
no condition set	
Add notes for administrator use	

Fig 3b: Home > Azure Information Protection > Labels > Label Name > Configure Condition

- o Admins will be able to view conditions in read-only mode.
- o Admins will not be able to edit condition settings.

🗄 Save 🗙 Discard 📋 Delete										
hoose the type of condition ①										
Information types Custom										
hoose an industry										
All Financial Medical and Health Privacy										
elect information types										
O Search to filter items										
Name										
ABA Routing Number										
Argentina National Identity (DNI) Number										
Australia Bank Account Number										
Australia Driver's License Number										
Australia Medical Account Number										
Australia Passport Number										
Australia Tax File Number										
Azure DocumentDB Auth Key										
Azure IAAS Database Connection String and Azure SQL Connection String										
Azure IoT Connection String										
	1	2	3	4	5 6	7	8	9	10 <	>
linimum number of occurrences										
1										

### 4) Admin tries to edit policies in the AIP portal

- Admins will not be able to add new policies.
- Admins will only be able to view the policy.
- Admins will not be able to save or delete policies.

#### Fig 4: Home > Azure Information Protection > Policies > Policy

Home > Azure Information Protection Azure Information Prot	ection   Policies		×
General	A This page is read-only, and current values cannot be modified.		
Quick start	Azure Information Protection labeling and policy management in the Azure Portal, as well as th longer be released for the classic client.	he Azure Information Protection classic client, reached end-of-life on April 1, 2021. Your current labels and labeling policies will continue to function as configured; however, no further support is provided	1. and maintenance versions will no $\rightarrow$
Analytics	To make changes to your labels and labeling policies, you must migrate to unified labeling and	d upgrade to the unified labeling client.	
usage report (Preview)			
& Activity logs (Preview)	Configure administrative name and description for each policy		
Data discovery (Preview)	configure automation in an accuration for each pointy		
I Recommendations (Preview)	Policy	Description	
Classifications	Global	Default policy for all users in the tenant	
Labels	Local Policy		
Policies			
Scanner			
D1 Clusters			

### 5) Admin tries to edit policies (export, advance settings)

- Admins will not be able to add new policies.
- Admins will be able to select the ellipsis (...) and right-click each to manage a policy. Admins will be able to select the **Export** and **Advanced settings** options.
- In the ellipses link (...), the Move up/down and Delete options will not be available.

Fig 5: Home > Azure Information Protection > Policies > Policy

Home > Azure Information Protection	0		
Azure Information Pro	otection   Policies		×
,O Search (Ctrl+/) «			
General	A This page is read-only, and current values cannot be modified.		
Quick start	Azure Information Protection labeling and policy management in the A	aure Portal, as well as the Azure Information Protection classic client, reached end of-life on April 1, 2021, Your current labels and labeling policies will continue to function as configured; however, no further support is provided, and maintenance versions will	Ino ->
Analytics	To make changes to your labels and labeling policies, you must migrate	to unified labeling and unorsele to the unified labeling client.	
Lat Usage report (Preview)			
& Activity logs (Preview)			
Data discovery (Preview)	Configure administrative name and description for each policy		
III Recommendations (Preview)	Policy	Description	
Classifications	Global	Default policy for all users in the tenant	
Labels	Local Policy	Export	
		Advanced settings	
Scanner			
Clusters			
Nodes			

# 6) Admin tries to add users to policies

- Admins will be able to view users.
- Admins will not be able to add or remove users.

Fig 6a: Home > Azure Information Protection > Policies > Policy >

rosoft - Azure Information Protection			
E Columns 🔛 Save 🗙 Discard [	🗐 Delete 🛓 Export		
Configure administrative name, descri	ption and scope for this policy		
Policy name			
Local Policy			
Policy description			
A Selected users or groups get this polic	у. 📀		
All Company			
	Policy	Marking	Protection
Label display name	· · · · · · · · · · · · · · · · · · ·		
Public Configure settings to display and appl	Local Policy	ers	~
Label display name     Public Configure settings to display and appl Title Sensitivity	Local Policy	ers	~
Label display name Public Configure settings to display and appl Title Sensitivity Tooltip	Local Policy	ers	V
Label display name Public Configure settings to display and appl Title Sensitivity Looltip The current label for this content. This s inside or outside the organization.	Local Policy y on Information Protection and us retting identifies the risk to the busine	ers ss if this content is shar	ed with unauthorized people
Label display name  Public  Configure settings to display and appl title Sensitivity fooltip  The current label for this content. This s inside or outside the organization.  Select the default label	Local Policy by on Information Protection and us setting identifies the risk to the busine	ers sx if this content is shar	ed with unauthorized people
Label display name Public Configure settings to display and appl Title Sensitivity Toohip The current label for this content. This i Inside or outside the organization. Select the default label None	Local Policy y on Information Protection and us uetting identifies the Hisk to the busine	ers ss if this content is shar	ed with unauthorized people.
Label display name     Public     Configure settings to display and appl     Title     Sensitivity     Tooltip     The current label for this content. This i     Inside or outside the organization.     Select the default label     None     Send logging data to Azure Information	Local Policy y on Information Protection and us setting identifies the risk to the busine Protection analytics ©	ers sx if this content is shar	ed with unauthorized people.
Label display name     Public     Configure settings to display and appl     Title     Sensitivity     Tooltip     The current label for this content. This i     Inside or outside the organization.     Select the default label     None     Send logging data to Azure Information     Off Not configured	Local Policy y on Information Protection and us setting identifies the risk to the busine Protection analytics Q	ers as if this content is shar	ed with unauthorized people
Label display name     Public     Configure settings to display and appl     Title     Sensitivity     Tootip     The current label for this content. This t     Inside or outside the organization.     Select the default label     None     Send logging data to Azure Information     Of    Not configured     All documents and emails must have a label	Local Policy y on Information Protection and us setting identifies the risk to the busine Protection analytics @ bel (applied automatically or by users)	ers as if this content is shar	ed with unauthorized people
Public      Configure settings to display and appl Title     Sensitivity      Tooltip      The current label for this content. This t     Inside or outside the organization.      Select the default label      None      Send logging data to Azure Information     Off Not configured  All documents and emails must have a la      Off On	Local Policy  y on Information Protection and us  retting identifies the risk to the busine  Protection analytics  o the (applied automatically or by users)	ers ss if this content is shar	ed with unauthorized people

Fig 6b: Home > Azure Information Protection > Policies > Policy > Select which users or groups get this policy.

icy: Local Policy			
Columns 🔄 Save 🗙 Discard 🗎 Delete 🛓	Export		
infigure administrative name, description and scop	e for this policy		
ical Policy ficy description			
Selected users or groups get this policy. ①			
III Company	Policy	Marking	Protection
Dublic	Local Policy		~

# 7) Admin tries to edit advanced setting configuration in the AIP portal

- Admins will be able to view settings in read-only mode.

- Admins will not be able to add new settings or remove settings.

Fig 7: Home > Azure Information Protection > Policies > Policy > Advanced Settings

Name	Value	
DisableDNE	falce	
EnableAudit	false	
EnableCustomPermissions	true	
HideBarByDefault	false	

## 8) Admin tries to activate protection in the AIP portal

- Admins will only be able to see the status (activated / deactivated).
- Admins will not be able to activate / deactivate.

Fig 8: Home > Azure Information Protection > Protection Activation

Home > Azure Information Protection Azure Information Prot	tection   Protection activation	×
P Search (Ctrl+/) «	Deschate	
General	▲ This pape is read-only, and current values connot be modified.	
G Quick start	Approx Information Protections taking and policy management in the Appre Portial as well as the Appre Portial as well as the Appre Total cast information Protection classic cleent reached end-of-life on April 1 2021. Toor current taking policies will continue to Anadon as configured however, no further apport is provided, and maintenance versions will no however the Interest for the Cast Configured however, no further apport is provided, and maintenance versions will no however the Interest for the Cast Configured however, no further apport is provided, and maintenance versions will no however the Interest for the Cast Configured however, no further apport is provided, and maintenance versions will no however the Interest for the Cast Configured however, no further apport is provided, and maintenance versions will no however the Interest for the Cast Configured however, no further apport is provided, and maintenance versions will no however the Interest for the Cast Configured however, no further apport is provided, and maintenance versions will no how the Interest for the Cast Configured how eversion of the Cast Configured how	->
Analytics	- To Takke changes to your labels and labeling policies, you must migrate to unfied labeling and upgrade to the unified labeling client.	
Lt. Usage report (Preview)		
& Activity logs (Preview)	Protection activation status	
Data discovery (Preview)	The control on status is estimated	
II Recommendations (Preview)	Ine processor subs a caseware. Protection must be advanted to comfigure labels that set permissions or to enable Office Information Rights Management (RM) protection for Exchange or SharePoint.	
Classifications		
Labels		
2 Policies		

### 9) Admin tries to edit protection templates in the AIP portal

For customers that are working with protection templates instead of labels, Admins could manage the protection templates from the portal. Moving forward:

- Admins will be able to view protection templates in read-only mode.
- Admins will not be able to edit / change protection settings in the AIP Portal.
- Admins can use <u>AIP PowerShell cmdlets</u> to edit protection.
- Admin will not be able to convert templates to labels using the portal but can still use PowerShell command

#### Fig 9: Home > Azure Information Protection > Labels

Label display name	Policy	Marking	Protection
Non-Business HD			
Public HD			
General HD			
Confidential HD			
scoped			$\checkmark$
> Protection templates			

### 10) Admin tries to edit protection in the AIP portal

- Admins will be able to view protection in read-only mode.
- Admins will not be able to edit / change protection settings in the AIP Portal.
- Admins can use <u>AIP PowerShell cmdlets</u> to edit protection.

Fig 10: Home > Azure Information Protection > Labels > Label Name > Protection Settings

Home > Azure Information Protection >	> Label: 2 >	
Protection		
Microsoft - Azure Information Protection		
Protection settings		
2		
Azure (cloud key) HYOK (AD RMS)		
Salact the protection action type (1)		
Set nermissions		
Set user-defined nermissions (Preview)		
Users	Permissions	
IPC_USER_ID_OWNER	Co-Owner	
Never By date By days		
Never By date By days		
Never By date By days		
Never By date By days		
Never By date By days		
Never By date By days		
Never By date By days Allow offline access Balance security requirements (includes acc	tess after revocation) with the flexibility to open protected content without an Internet	
Never By date By days Allow offline access Balance security requirements (includes acc connection. More information and recomme	tess after revocation) with the flexibility to open protected content without an Internet ended settings	
Never By date By days Allow offline access Balance security requirements (includes acconnection. More information and recommendations) Always Never By days	tess after revocation) with the flexibility to open protected content without an Internet ended settings	
Never         By date         By days           Allow offline access         Balance security requirements (includes acconnection. More information and recommon an	tess after revocation) with the flexibility to open protected content without an Internet ended settings	
Never         By date         By days           Allow offline access           Balance security requirements (includes acconnection. More information and recommon Always           Never         By days           Protection template ID - 0ee8cd87-2956-46	tess after revocation) with the flexibility to open protected content without an Internet ended settings 58b-a820-115a5f61700c	
Never         By date         By days           Allow offline access           Balance security requirements (includes acconnection. More information and recommon and recom	tess after revocation) with the flexibility to open protected content without an Internet ended settings 58b-a820-1f5a5f61700c	
Never         By date         By days           Allow offline access           Balance security requirements (includes acconnection. More information and recommodiate informatinte informatinte information andinte informatinte informatinte inf	tess after revocation) with the flexibility to open protected content without an Internet lended settings 58b-a820-1f5a5f61700c	
Never By date By days Allow offline access Balance security requirements (includes acc connection. More information and recomm Always Never By days Protection template ID - 0ee8cd87-2956-46	tess after revocation) with the flexibility to open protected content without an Internet ended settings 58b-a820-1f5a5f61700c	
Never By date By days Allow offline access Balance security requirements (includes acc connection. More information and recomm Always Never By days) Protection template ID - 0ee8cd87-2956-46	tess after revocation) with the flexibility to open protected content without an Internet ended settings 58b-a820-1f5a5f61700c	
Never By date By days Allow offline access Balance security requirements (includes acconnection. More information and recommendation) Always Never By days Protection template ID - 0ee8cd87-2956-46	tess after revocation) with the flexibility to open protected content without an Internet rended settings 58b-a820-1f5a5f61700c	
Never By date By days Allow offline access Balance security requirements (includes acconnection, More information and recommendation) Always Never By days Protection template ID - 0ee8cd87-2956-46	tess after revocation) with the flexibility to open protected content without an Internet lended settings 58b-a820-1f5a5f61700c	
Never By date By days Allow offline access Balance security requirements (includes acco connection. More information and recommon Always Never By days Protection template ID - 0ee8cd87-2956-466	tess after revocation) with the flexibility to open protected content without an Internet ended settings 58b-a820-1f5a5f61700c	
Never By date By days Allow offline access Balance security requirements (includes acc connection. More information and recomm Always Never By days) Protection template ID - 0ee8cd87-2956-46	tess after revocation) with the flexibility to open protected content without an Internet lended settings 58b-a820-1f5a5f61700c	
Never By date By days Allow offline access Balance security requirements (includes acco connection. More information and recomm Always Never By days) Protection template ID - 0ee8cd87-2956-46	tess after revocation) with the flexibility to open protected content without an Internet ended settings 58b-a820-1f5a5f61700c	
Never By date By days Allow offline access Balance security requirements (includes acc connection. More information and recomme Always Never By days Protection template ID - 0ee8cd87-2956-46	tess after revocation) with the flexibility to open protected content without an Internet rended settings 58b-a820-1f5a5f61700c	
Never By date By days Allow offline access Balance security requirements (includes acco connection. More information and recommon Always Never By days Protection template ID - 0ee8cd87-2956-46	tess after revocation) with the flexibility to open protected content without an Internet rended settings 58b-a820-1f5a5f61700c	
Never By date By days Allow offline access Balance security requirements (includes acco connection. More information and recommon Always Never By days Protection template ID - 0ee8cd87-2956-466	cess after revocation) with the flexibility to open protected content without an Internet ended settings 58b-a820-1f5a5f61700c	
Never         By date         By days           Allow offline access         Balance security requirements (includes acconnection. More information and recommon Always         Never         By days           Always         Never         By days         Never         Protection template ID - 0ee8cd87-2956-46	tess after revocation) with the flexibility to open protected content without an Internet ended settings 58b-a820-1f5a5f61700c	

### 11) Admin tries to add, import, delete languages in the AIP portal

- Admins will only be able to export language settings.
- Admins will not be able to add, import, or delete languages.

Fig 11: Home > Azure Information Protection > Languages

Home > Azure Information Protection       Azure Information Protection   Languages				
,⊅ Search (Ctrl+/) ≪				
General	A This page is read-only, and current values cannot be modified.			
Quick start	Anal Information Proceeding and policy management in the Azure Proti. as well as the Azure Information Protection dusic cliefs ranched and of clie on April 1. 2021. Your current labels and labeling policies will centime to function as configured however, no Anther support is provided. And maintenance versions will no $\rightarrow$			
Analytics	Anyone we investigate the second			
La Usage report (Preview)				
& Activity logs (Preview)	Specify supported languages			
Data discovery (Preview)	Learn More			
III Recommendations (Preview)	Language name	Last modified		
Classifications	Arabic (Saudi Arabia)	2/2/2021		
Labels	🗾 Bulgarian (Bulgaria)			
Policies	Chinese (Simplified, PRC)			
Scanner				

### 12) Admin tries to activate/deactivate unified labeling in AIP portal

- Admins will be able to activate unified labeling from the AIP portal.
- Admins will be able to copy policies to the Microsoft 365 Compliance center.
- Admins will not be able to publish policies in the AIP portal.

### Fig 12a: Home > Azure Information Protection > Unified Labeling > Activate

Home > Azure Information Protection	n Protection   Unified labeling ×
P Search (Ctrl+/) e	Actives # Actives # An Anti-Active Active
General	▲ This page is read-only, and current values cannot be modified.
Co Quick start	Apple Information Protection balling and policy management in the Apple Rotal, as will at the Apple Information Protection datasic detert, reached and of-life on Appl 1. 2021, Your current balling policies will confuse to function as configured, however, no further support is provided, and maintenance versions will no hopping is a reason of the function as a configured however, no further support is provided, and maintenance versions will no the configured as a support of the apple of the apple of the configured however, no further support is provided, and maintenance versions will no To main characteristic to use Information and incomestion to use of the the apple of t
La Usage report (Preview)	
B2 Activity logs (Preview)	Unified labeling status
Data discovery (Preview)	Unified labeling. Not activated. Unified labeling is not activated for this tenant, As a result, Asure Information Protection labels are limited to the Asure Information Protection classic client. To make your labels available for clients and services that support unified labeling and in the Microsoft 165 Compliance center, select Activate.
Classifications	United adversing is a requirement for the Apple montandom interfaced and adverse, but - multi-adverse for United adverse for an articipation with share-out and rower B.
Labels	To us samy accurate uniting and compare to be your coase, comma does many you apprave to the unities usering colema, and unities usering colema and apprave.
Policies	Laboring and policy management in the ALMP portal Records are on-on-one of Aprin 1, 2021. Your current based is and baseling policies will contains or and injurity however, no future support is provided, and maintenance versions will no longer be released for the classic client. To make changes to your labels and labeling policies, you must migrate to unified labeling and upgrade to the unified
Scanner	labeling client. Learn more.
Clusters	
Nodes	
Network scan jobs (Preview)	

Fig 12b: Home > Azure Information Protection > Unified Labeling >

Home > Azure Information Protection	n
Azure Information	Protection   Unified labeling
,0 Search (Ctrl+/) «	b Activite <sup>1</sup> / <sub>10</sub> in Adda <sup>1</sup> / <sub>10</sub> Copy paticies
General	▲ This page is read-only, and current values cannot be modified.
Quick start	April Information Testication Labeling and policy management in the April Potski and mail as the April Information Potencies Casic Celert, mached and ed-life on April 1.2221. You current labels and balang policies will continue to function as configured Potencies no further support is provided and maintenance versions will no based to the maintenance Tort Resistance Version State Celert
Analytics	To make changes to your labels and labeling policius, you mutt regrate to unified labeling and upgrade to the unified labeling client.
LL Usage report (Preview)	
& Activity logs (Preview)	Unified labeling status
Data discovery (Preview)	Differ Unified Andread
III Recommendations (Preview)	
Classifications	Unitive useling a activate for this tensing, and you can manage your uses in the microsoft ass comparate center, ine wates can be used by the Aute information instruction cient and by united abeling cients.
<ul> <li>Labels</li> </ul>	Secretaria and a secret
D Policies	Conditions configured for labels in the Acces provid apply in the Acces Information Protection district class (at cost). Effected to end (at cost) and (at labels) in the Accessional protection (at cost).
Scanner	Tablics and address sectors and address to address the sector of the sec
Clusters	
Nodes	Important
C Network scan jobs (Preview)	You can also use built-in labels to protect documents and emails in the latest Office apps. Supported apps include Word, PowerPoint, Excel, and Outlook, in platforms on the web, Windows, Mac 103, and Android. Built-in labels are also supported on other productivity services where information resides, such as
Pp Content scan jobs	ShareFort Online, Exchange Online, and Yower BL
P Repositories (Preview)	We recommend that you turn on the salt(b) in Shareboart Online PowerShell to get rich collaboration experience and enable data protection features based on sensitive labels in Power 81.
Manage	
Configure analytics (Preview)	

## 13) Using the AIP classic client

- Users will be able to apply label and protection and to consume protected files.
- The AIP classic client is out of support.
- Maintenance versions for the AIP classic client will not be released.

#### 14) AIP labels in Microsoft Cloud App Security

- Microsoft Cloud App Security will not support AIP labels after March 31<sup>st</sup>, 2021. Only unified labels will be supported.
- Existing policies in Microsoft Cloud App Security will not apply or discover AIP labels in files. An alert will be sent to the admin in case the policy had AIP labels.
- Microsoft Cloud App Security will support only unified label for policies and for labels discovery.

### Managing labels and policies in the Microsoft 365 Compliance center

#### Fig 14a: Microsoft 365 compliance > Solutions > Information Protection > Labels >

After you activate and migrate to unified labeling, your labels will be available in the Microsoft 365 Compliance center.

- Moving forward, you can manage your labels and policies in the Microsoft 365 Compliance center.
- For more information about creating, managing labels and policies in the Compliance center, see the <u>Microsoft 365 compliance documentation</u>.

III Microsoft 365 compliance	©	? (BG)
▲ Alerts		<b>^</b>
✓ Reports	Information protection - Show in navigation	on
Policies	Labels Label policies Auto-labeling	- 1
S Permissions	New feature in preview	- 1
Solutions		- 8
田 Catalog	Extend labeling to assets in	- 8
🖻 Audit	Azure Purview	- 8
	When you turn on labeling for Azure Purview, you'll be able to apply your	- 1
G Communication compliance	Microsoft 365 sensitivity labels to assets such as SQL columns, files in Azure Blob Storage, and more. Learn more about labeling for Azure Pundem	- 1
Data loss prevention		- 1
🗅 Data subject requests	lum on	- 3
盦 eDiscovery ~	Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settions you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites	
Information governance	Learn more about sensitivity labels	- 1
🔓 Information protection	① You can now create sensitivity labels with privacy and access control settings for Teams. SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.	
P <sub>A</sub> Insider risk management	🕂 Create a label 📮 Publish labels 🖒 Refresh	~

Fig 14b: Microsoft 365 compliance > Solutions > Information Protection > Label policies >

::: Microsoft 365 compliance				@? BG
✓ Reports				
Delicies	Information protection			🔊 Remove from navigation
S Permissions	Labels Label policies Auto-labeling			
Solutions	Create sensitivity label policies to publish one or m	nore labels to your users' Office apps (like Outlook	< and Word), SharePoint sites, and Office 365 grou	ups. Once published, users can apply the
🛱 Catalog		ensitivity laber policies		d items
🖹 Audit				4 items
	Name	Created by	Last modified	
Communication compliance	Global Policy	MOD Administrator	Feb 25, 2021 9:35 PM	
Data loss prevention	Test Policy	Gopal	Jan 28, 2021 5:46 AM	
Data subject requests	Alex's Policy	Alex Steele	Feb 25, 2021 9:43 PM	
💼 eDiscovery 🗸 🗸	BabylonTest	Hen	Jan 5, 2021 10:46 PM	
Information governance				
🔓 Information protection				
$\mathcal{P}_{\!\!\Delta}$ Insider risk management				

# AIP portal and classic client admin user experience summary

#	Admin Experience	Not Impacted	Impacted
1	Admin tries to add new label.		Admin will not be able to add a new label.

			Admin will not have the shortcuts or any right-click options.
2	Admin tries to edit a label	Admin will be able to view a label in read-only mode.	Admin will not be able to edit or delete label content and settings
3	Admin tries to edit label conditions	Admin will be able to view conditions in read-only mode.	Admin will not be able to edit conditions
4	Admin tries to edit policy	Admin will be able to only view policy	Admin will not be able to save or delete a policy.
5	Admin tries to edit policies (export, advance settings)	Admin will be able to select the ellipsis and right-click options to manage each policy. Admins will be able to select <b>Export</b> and <b>Advanced settings</b> buttons.	Admin will not be able to add new policy. In the shortcut, the link will not have move up/down or delete options.
6	Admin tries to add user	Admin will be able to view users	Admin will not be able to add a user or remove a user
7	Admin tries to edit advanced	Admin will be able to	Admin will not be able to add
8	Admin tries to activate protection	Admin will be able to see the status (activated / deactivated)	Admin will not be able to activate / or deactivate
9	Admin tries to edit protection templates in the AIP portal	Admins will be able to view protection templates in read- only mode. Admins can use AIP PowerShell cmdlets to edit protection.	Admins will not be able to edit / change protection settings in the AIP Portal. Admin will not be able to convert templates to labels using the portal but can still use PowerShell command
10	Admin tries to edit protection	Admin will be able to view protection in read-only mode.	Admin will not be able to edit protection
11	Admin tries to add, import, delete language	Admin will be able to only export	Admin will not be able to add, import, delete
12	Admin tries to activate unified labeling	Admin will be able to activate and copy the policy	Admin will not be able to publish labels in the AIP portal
13	End users using classic client	Users will be able to apply labels and protection and to consume protected files	AIP classic is out of support. Maintenance versions will not be released.
14	AIP labels in Microsoft Cloud App Security		AIP labels will not be supported. Only unified labels will be supported.

# Some important links about unified labeling

- Deprecation notice for sunsetting label management in the Azure portal and AIP client (classic)
- Understanding Unified Labeling migration
- Identify the Office 365 versions that support unified labeling
- How to migrate Azure Information Protection labels to unified sensitivity labels?
- Where can I find information to compare labeling clients?
- How to install unified labeling clients?
- What is the user experience across platforms?
- How do I file for a support extension?

### Top 5 frequently asked questions

- 1. How can I find my status on extended support?
  - CSS will be able to assist you to find status on extended support.
- 2. How to request for extended support?
  - You can request extended support using the form posted <u>here</u>.
- 3. What are the requirements for requesting extended support?
  - Provide details of feature/functionality that is blocking your migration.
- 4. Who should I contact regarding migration questions?
  - There are various channels. Yammer, CSS, or your CXE representative.
- 5. What is the SLA for reviewing the extended support request?
  - The SLA for reviewing extended support requests is 2-3 weeks. We will provide an approval or reject response or will request for additional information to assess the situation.