File Protection Solutions in Office 365

Recommended architectures for protecting files in Office 365

This topic is 1 of 5 in a series 1 2 3 4

Three types of data

1 Baseline data

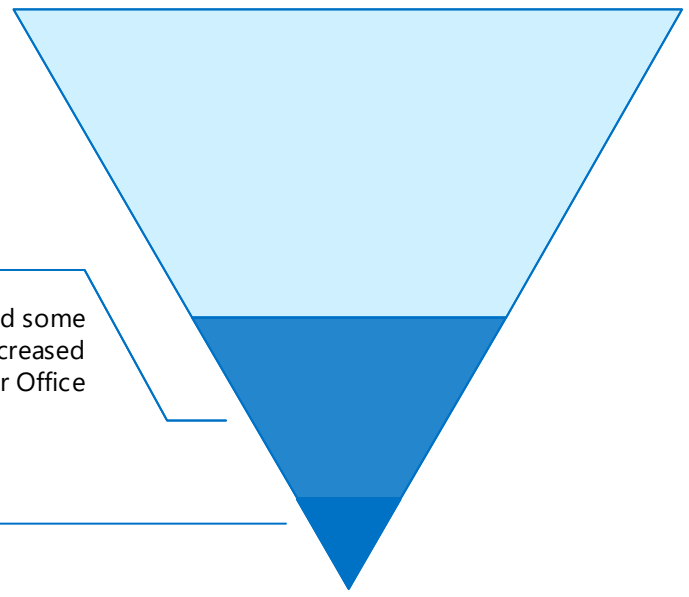
Microsoft recommends you establish a minimum standard for protecting data, as well as the identities and devices that access your data. Microsoft provides strong default protection that meets the needs of many organizations. Some organizations require additional capabilities to meet their baseline requirements.

2 Sensitive data

Some organizations have a subset of data that needs to be protected both internally and externally from accidental oversharing and leakage. Examples include executive strategy plans, product specifications, files with personally identifiable information, and some categories of regulated data. Apply increased protection to targeted files within your Office 365 environment.

3 Highly regulated or classified data

Some organizations may have a very small amount of data that is highly classified, trade secret, or regulated data. Microsoft provides capabilities to help organizations meet these requirements, including added protection for identities and devices.



File protection capabilities

Microsoft provides a range of capabilities to protect your data. This document describes capabilities for protecting files so you can choose the best options to protect your organization's data.

Baseline protection	Increased data protection	Protection for highly regulated data
Default file encryption	Classification, labeling, and protection	Bring Your Own Key (BYOK) with Azure Information Protection and SharePoint Online
Permissions for SharePoint and OneDrive for Business libraries	Data Loss Prevention (DLP) in Office 365	Hold Your Own Key (HYOK) with Active Directory Rights Management Service and SharePoint Online
External sharing policies	Office 365 service encryption with Customer Key (coming soon)	
Device access policies for SharePoint Online and OneDrive for Business	Windows 10 capabilities: Bitlocker and Windows Information Protection (WIP)	

Capabilities are additive →

Identity and device capabilities

Microsoft recommends protecting your identities and devices at similar levels that you protect your data. These capabilities can be used together with file protection capabilities. For more information, see Identity and Device Protection for Office 365.

Baseline protection	Increased protection	Protection for highly regulated data
Intune mobile application management	Intune device management	
Azure Active Directory multi-factor authentication		
	Azure Active Directory conditional access	
Azure Active Directory Identity Protection		
	Microsoft Cloud App Security -or- Office 365 Advanced Security Management	
	Azure Active Directory Privileged Identity Management	

See topics 2-4 for more information and resources.

April 2017

Microsoft

File Protection Solutions in Office 365

Recommended architectures for protecting files in Office 365

Baseline protection

This topic describes capabilities you can use to increase the baseline level of protection of files in Office 365. Some of these capabilities apply broadly. Some of these capabilities can be targeted to specific data sets.

Default file encryption

By default, all files stored in Office 365 are encrypted with the strongest encryption and detection technologies available. This protects files from attackers and people outside of your organization.

Protection of files in transit

Every file in SharePoint and OneDrive is encrypted in transit (TLS 1.0, 1.1, and 1.2) between the user's browser, PC, Mac, or mobile device and our datacenters. All connections are established using 2048-bit keys.

This applies to protocols on any device used by clients, such as Skype for Business Online, Outlook, and Outlook on the web.

More information:

Whitepaper download: File Security in Microsoft Office 365

Microsoft Trust Center — Encryption

Protection of files in the datacenter

Once the file reaches the Microsoft datacenter, the files are encrypted through two components: BitLocker disk-level encryption and per-file encryption. BitLocker encrypts all data on a disk. Per-file encryption goes even further by including a unique encryption key for each file. Further, every update to every file is encrypted using its own encryption key. Before they're stored, the keys to the encrypted files are themselves encrypted and stored in a physically separate location.

Every step of this encryption uses Advanced Encryption Standard (AES) with 256-bit keys and is Federal Information Processing Standard (FIPS) 140-2 compliant. The encrypted content is distributed across several containers throughout the datacenter, and each container has unique credentials.

For more information about encryption used by Microsoft cloud services and datacenters, see the Data Encryption in OneDrive for Business and SharePoint Online.

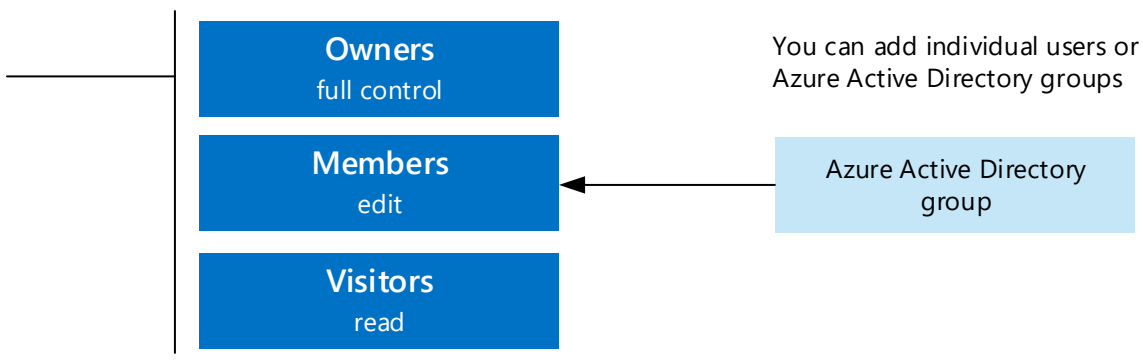
Permissions for SharePoint and OneDrive for Business libraries

You can use permissions in SharePoint to provide or restrict user access to the site or its contents.

Default SharePoint groups

SharePoint sites come with several default groups that you can use to manage permissions.

These are not related to Office 365 groups.



Create a custom group for finer-grain control

Custom groups in SharePoint Online let you choose finer-grain permission levels. You can also determine who can view the membership of the group and whether users can request to join the group.

Full Control	Design	Edit	Contribute	Read	View Only
	Contribute + approve and customize	Contribute + add, edit and delete lists (not just list items)	View, add, update, delete list items and documents	View and download	View, no download

More information:

Understanding permission levels in SharePoint

Understanding SharePoint groups

Office 365 Groups and Microsoft Teams

In addition to configuring the default permissions for a SharePoint site, you can take advantage of Office 365 Groups or Microsoft Teams.

Office 365 private group

Content in a private group can only be seen by the members of the group. People who want to join a private group have to be approved by a group owner.

Groups cannot be seen or accessed by people outside of your organization unless those people have been specifically invited as guests.

Learn about Office 365 Groups

Microsoft Teams

Microsoft Teams is the chat-centered workspace in Office 365. Currently Microsoft Teams are all private. When a new team is created, a new Office 365 Group is also created, including the group SharePoint site

Chat data is encrypted in transit and encrypted at rest. Files are stored in a group SharePoint library and restricted to members of the team.

Administrator settings for Microsoft Teams

For users—Microsoft Teams Quick Start

Continued on next page

External sharing policies

Be sure to configure external sharing policies to support your collaboration and file protection objectives.

An external user is someone outside of your organization who is invited to access your SharePoint Online sites and documents but does not have a license for your SharePoint Online or Microsoft Office 365 subscription.

Some polices can be set for individual site collections. This can help you protect sensitive files at a higher level than other files. However, policies for individual site collections cannot be less restrictive than what is set for the entire SharePoint Online environment.

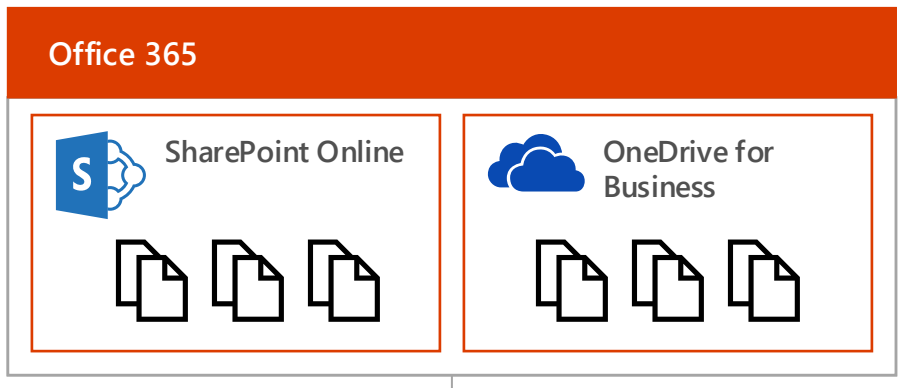
Manage external sharing for your SharePoint Online environment

Share sites or documents with people outside your organization

External sharing policies apply to both SharePoint Online and OneDrive for Business.

You must be a SharePoint Online admin to configure sharing policies.

You must be a Site Owner or have full control permissions to share a site or document with external users.



Type of sharing

- Don't allow sharing outside your organization
- Allow sharing to authenticated external users only (allow new or limit to existing)
- Allow sharing to external users with an anonymous access link
- Limit external sharing using domains (allow and deny list)
- Choose the default link type (anonymous, company shareable, or restricted)

These policies can be set for individual site collections.

What external users can do

- Prevent external users from sharing files, folders, sites they don't own
- Require external users to accept sharing invitations with the same account the invitation was sent to

Notifications

Currently only available in OneDrive for Business. Notify owners when:

- Users invite additional external users to shared files
- External users accept invitations to access files
- An anonymous access link is created or changed

Device access policies for SharePoint Online and OneDrive for Business

Conditional access and network location policies let you determine whether access to data is limited or blocked.

The device-based policies require Microsoft Intune (or another mobile device management tool) and Azure Active Directory Premium P1. The network location policy does not require additional licensing.

Network location policy (in preview) — You can configure network location policies both in SharePoint admin center and in Azure Active Directory. Azure Active Directory enforces this policy at sign in. Office 365 enforces this policy when resources are accessed. You can configure this in one or both places. There is no dependency for configuring this in SharePoint admin center.

Azure Active Directory — The device based policies require two conditional access rules in Azure AD. These rules can be targeted to specific user groups, otherwise they apply tenant-wide.

Microsoft Intune — Intune or another mobile device management tool is required to enforce device compliance requirements. Devices must be enrolled. Other mobile device management tools can only enforce these conditional access rules for Windows 10 computers.

Settings apply tenant-wide unless conditional access policies in Azure Active Directory are targeted to specific users or groups.

The chart below summarizes the capabilities and dependencies.

Dependencies for using device access policies in SharePoint admin center

Objective	Only allow access from specific IP address locations	Prevent users from downloading files to non-domain joined devices	Block access on non-domain joined devices	Prevent users from downloading files to non-compliant devices	Block access on non-compliant devices
SharePoint admin center	✓	✓	✓	✓	✓
Azure Active Directory		✓	✓	✓	✓
Microsoft Intune				✓	✓

More information

SharePoint Online admin center: Control access from unmanaged devices

For information about implementing conditional access, see page two in this content: Identity and Device Protection for Office 365.

File Protection Solutions in Office 365

Recommended architectures for protecting files in Office 365

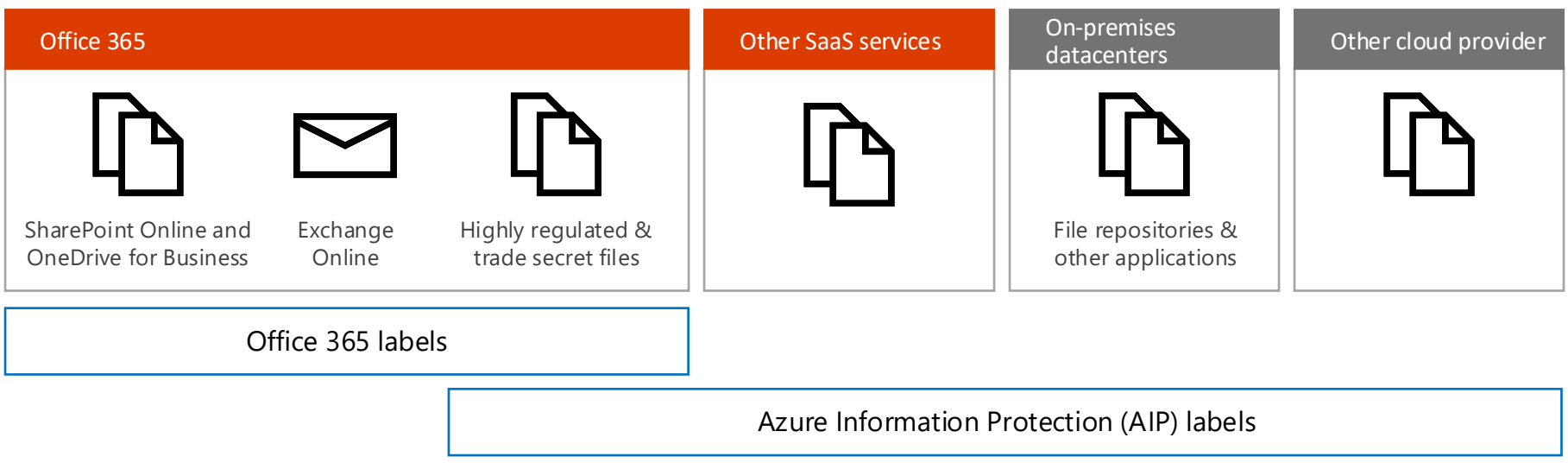
Sensitive data protection

This topic describes capabilities you can use to protect sensitive files in Office 365. Some of these capabilities apply broadly. Some of these capabilities can be targeted to specific data sets.

Classification, labeling, and protection

Microsoft recommends you classify and label your data. Microsoft capabilities make it easy for your organization to classify and label data in intuitive ways based on the source, context, and content of the data. Classification can be fully automatic, user-driven, or both. Once data is classified and labeled, protection can be applied automatically on that basis.

Today labels can be created in Office 365 and Azure Information Protection. These solutions complement each other to provide full protection through the data lifecycle, starting as data is born and stored and persisting as data travels. Start today, leverage both capabilities. Over time these technologies will converge into a unified labeling and classification engine and you will be able to achieve even more.



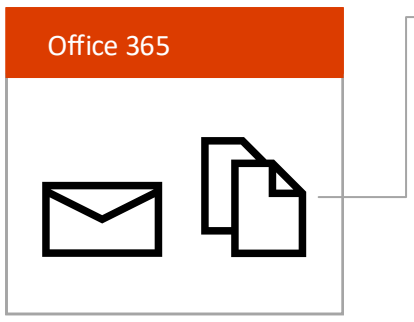
Protecting files in Office 365

You can use both types of labels for files in Office 365. These labels can be used together for increased protection.

Start with Office 365 labels

Use Office 365 labels for files and mail in Office 365.

- Users can manually apply labels.
- SharePoint libraries can automatically assign labels.
- DLP rules can automatically assign labels.
- DLP rules can take action based on labels, such as blocking mail or files from being shared externally.



Add Azure Information Protection to make sure your data remains protected and your polices are honored as files travel outside of Office 365

Azure Information Protection labels can be additionally applied to files that require protection that travels with the files and persists outside of Office 365.

- Any type of file that require protection or policy compliance inside and outside of your org, such as visual markings, encryption, and permissions.
- Files that are shared across SaaS applications.
- Files stored on-premises or with other cloud providers.

Office 365 DLP rules can also be used to take action based on these labels.

Continued on next page

More information

	Office 365 labels	Azure Information Protection labels
Recommended use cases	Retention and Office DLP.	Sensitivity protection and persistency across apps and environments.
Applying labels	Choose labels from the document panel in SharePoint Online and OneDrive for Business. For mail, apply labels directly from Outlook 2016, Outlook 2013, or Outlook Web Access. Use Office 365 DLP rules to automatically find and label files. Configure SharePoint Online libraries to automatically label documents.	Choose labels within Office client apps from the Azure Information Protection client ribbon. The client works with Office versions 2010, 2013, and 2016. Azure Information Protection policies can be configured to automatically suggest or assign labels based on the contents of the file. Users can also classify files by using Windows File Explorer. Select a file, multiple files, or a folder. Right-click, and select **Classify and protect**. Additionally, administrators can use PowerShell with the client to efficiently label files in bulk on Windows computers and file shares. Similar support for SharePoint is coming soon. Azure Information Protection user guide Using File Explorer to classify and protect files Using PowerShell with the Azure Information Protection client
Protect and encrypt files	Use DLP rules to protect files based on labels. Protection does not currently include encryption.	Apply visual markings (such as watermarks) based on these labels. Use DLP rules in Office 365 to protect files based on labels. Use Azure Rights Management templates in Azure to automatically apply encryption based on labels. This protection includes defining rights for files. You can encrypt using the defualt service encryption key, your own key (Bring Your Own Key), or your own key that you hold on premises (Hold Your Own Key).
File type support	Office 365 labels work with all file types that are allowed by the service. Types of files that cannot be added to a list or library	File types supported by the Azure Information Protection client

Office 365 labels and data loss protection (DLP)

Office 365 labels are included with Office 365 E1, E3, and E5 plans for manual application by users. Automated labeling using data loss protection policies is a part of Office Advanced Data Governance and requires the Office 365 E5 plan or the Advanced Compliance standalone license.

Labels are available in SharePoint Online, OneDrive for Business, Outlook, Outlook Web Access, and Office 365 Groups.

Labels work with Office 365 data loss prevention (DLP). You can automate the application of labels and use DLP policies to protect data based on labels.

Automated labeling with DLP works across Exchange Online, SharePoint Online, and OneDrive for Business.

Office 365 labels

- Labels are created in the Security and Compliance Center.
- Publish labels to specific audiences (users or groups).
- Choose which locations to publish labels to—Exchange, SharePoint, OneDrive accounts, and Office 365 Groups.
- Users apply labels or you can automatically apply labels by using a query (KQL query language) or other condition.
- Add labels to DLP policy conditions.

SharePoint Online integration includes:

- Labels show up in the document panel where users can easily apply them.
- Use labels as a library column and group documents by classification label.
- Configure a library to automatically classify all documents with a specific label.

Automated DLP policies

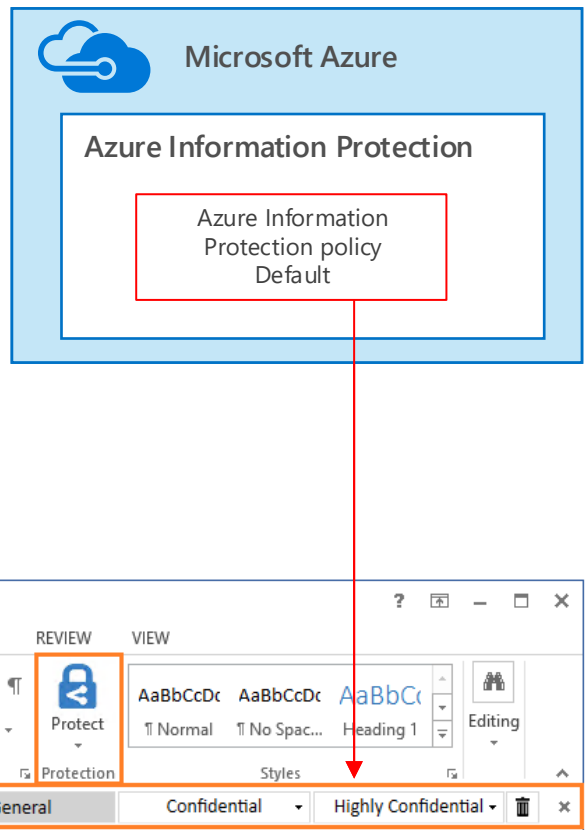
- Start with a template and identify what type of content to automatically detect and label, such as content with passport numbers or social security numbers.
- Apply the policy to all content in Office 365 or define specific locations. Specific locations include Exchange, SharePoint, and OneDrive accounts. You can choose specific SharePoint sites and OneDrive accounts.
- Detect when content is shared and determine what action to take. Actions include, block sharing, alert user that sharing is not allowed, allow the user to override the policy, and alert on the sharing.

More information:
New Office 365 capabilities help you proactively manage security and compliance risk

Continued on next page

Azure Information Protection classification and labeling

You can use Azure Information Protection with the Azure Information Protection client for classification and labeling. This requires a license that includes Azure Information Protection.



Default Azure Information Protection Policy

Labels are defined in an Azure Information Protection Policy. Microsoft recommends using the default policy and customizing this, if needed.

Here's how it works:

- Configured in Azure.
- Downloaded to the Azure Information Protection client.
- Includes five labels: Personal, Public, General, Confidential, and Highly Confidential.
- Labels determine how the file is classified and additional conditions or protections that are applied.
- You can customize labels and sub-labels and add new labels.

Decide what classification labels to apply to your sensitive data and update the labels to support your decision.

Azure Rights Management encryption

While Azure Information Protection works with Azure Rights Management to apply protection, you do not need to encrypt your sensitive data to protect it in Office 365. We don't recommend you encrypt Office 365 files using Azure Rights Management unless you have a business requirement that justifies the tradeoffs.

If Azure Rights Management encryption is applied to files in Office 365, the service cannot process the contents of these files. Co-authoring, eDiscovery, search, Delve, and other collaborative features do not work. Data loss prevention can take action based on labels, but not on the contents of the files.

Deployment

1. **Activate Azure Rights Management**
   If you have implemented IRM with SharePoint, this service is already activated.
   Activating Azure Rights Management
2. **Decide what classification label(s) to apply to your sensitive files**
   You can customize the default labels and add new labels.
   Default Azure Information Protection policy settings
3. **Update the labels to support your decisions**
   Reconfigure the default Azure Information Protection labels to make any changes you need to support your classification decisions.
   How to configure a label to apply Rights Management protection
4. **Get ready to train users**
   Produce user guidance that explains which label to apply and when.
   Azure Information Protection user guide
5. **Install the Information Protection client**
   You can script and automate the installation, or users can install the client manually.
   The client side of Azure Information Protection
   Installing the Azure Information Protection client

Using the solution

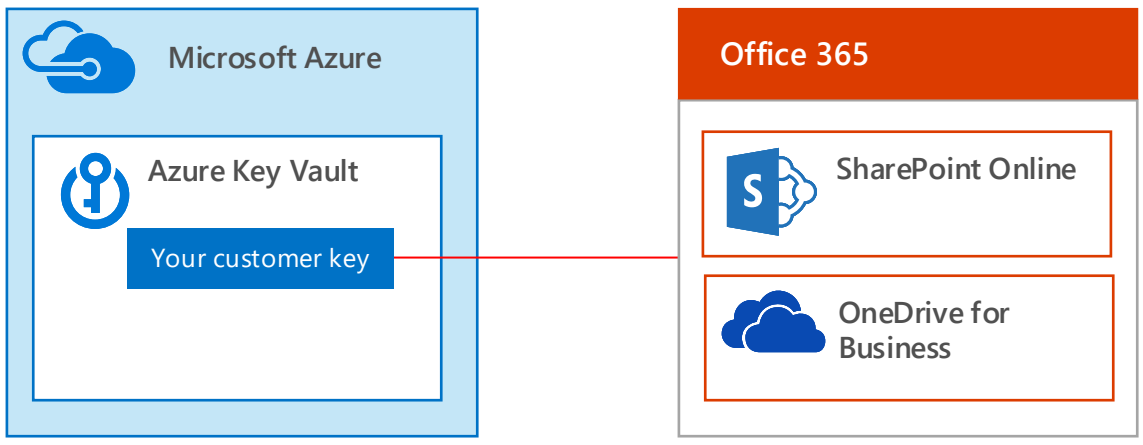
1. **Install the Information Protection client**
   If installation isn't automated, users can install the client manually.
   Download page for manual installation
2. **Use the client toolbar to apply labels**
3. **Upload files to the SharePoint library**
   Be sure users know which IRM-protected SharePoint library to use for your sensitive files.

Continued on next page

Office 365 service encryption with Customer Key

Coming soon. To help customers meet their compliance requirements, customers have the option to manage and control their own encryption keys for Office 365. Encrypting at the service level offers an added layer of protection for files in SharePoint Online and OneDrive for Business.

Customer Key is applied tenant-wide for all files in SharePoint Online and OneDrive for Business.



Deployment

1. **Create your own key vault in Azure**

   Create a hardened container (a vault) in Azure, to store and manage cryptographic keys and secrets in Azure.

   Get started with Azure Key Vault

2. **Add your key to the key vault**

   Generate your own key and transfer it to the Azure Key Vault or create it directly in the vault.

   Add a key or secret to the key vault

3. **Enable your key with Office 365**

   Authorize your Office 365 tenant to use the encryption key for files in OneDrive and SharePoint Online.

Windows 10 capabilities for file protection

A couple of Windows 10 capabilities contribute to file protection for Office 365 files. These capabilities require fully managed devices.

Bitlocker protects data when devices are lost or stolen

BitLocker Drive Encryption provides full disk encryption on Windows 10 PCs. If the device is lost or stolen unauthorized users can't gain access to files on the protected drives, including files synced from OneDrive for Business.

Bitlocker overview

Windows Information Protection (WIP) protects against data leakage

WIP separates work content from personal content and helps prevent accidental data leaks on enterprise-owned devices and personal Windows 10 devices that employees bring to work.

For example, WIP helps prevent a user from syncing or copying files in OneDrive for Business or SharePoint Online to a personal OneDrive or other personal cloud storage location. It also helps prevent a user from copying and pasting business content inside files or business apps to a non-business location, such as a personal document or a public website.

As an administrator, you can determine which apps are approved and have access to business content. You can also determine whether to block users from copying and pasting content to non-business locations or to just warn the user and audit the action.

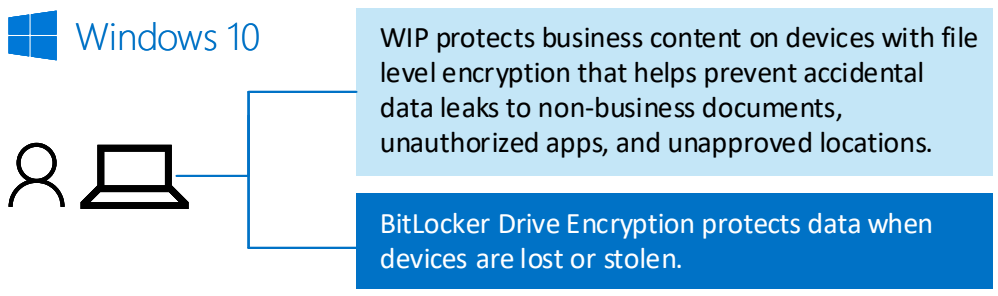
All content that is categorized as business content by WIP is encrypted. Here's how this works:

- Content that is downloaded to the device from a business location is automatically categorized as business content and encrypted.
- All new content created using business-only apps (such as a line of business app) is automatically categorized as business content and encrypted.
- New content created in dual purpose apps (apps used for both personal and business use, such as Word) is categorized by the user. Business content is encrypted when the content is saved to the device. Personal content is not encrypted.

On Windows 10 devices that use BitLocker, WIP provides an additional layer of protection. While BitLocker encrypts all data at rest on the device, WIP provides additional protection to your business content to help prevent accidental leaks. This includes copying files to removable media, such as a USB drive.

You can use WIP in combination with Office 365 data governance capabilities and Azure Information Protection. WIP protects against the most common accidental leaks while Office 365 and Azure Information Protection provide advanced protection capabilities. For example, you can use automated DLP rules to protect files that are e-mailed outside of your organization.

Protect your enterprise data using Windows Information Protection (WIP)



File Protection Solutions in Office 365

Recommended architectures for protecting files in Office 365

Highly regulated or classified data protection solutions

A few organizations require protection for a small subset of data that is classified or highly regulated. Microsoft provides advanced capabilities to help organizations meet these requirements while taking advantage of cloud storage and other cloud-based information protection capabilities.

These solutions allow you to protect targeted data sets at much higher levels than other data in your organization.

Choose one of these options:

- Bring Your Own Key (BYOK) with Azure Information Protection and SharePoint Online — all components are cloud-based. Apply protection before or after uploading files to SharePoint Online.
- Hold Your Own Key (HYOK) with Active Directory Rights Management Service (on-prem product) and SharePoint Online — this is a hybrid solution. Use HYOK and RMS to encrypt files on premises before uploading them to a SharePoint site.

Because of the complexity, implement the HYOK solution only if the BYOK solution does not meet your requirements.

Both of these options can be used with an Office 365 private group or Microsoft Teams to manage permissions to these files and to limit who can see these libraries.

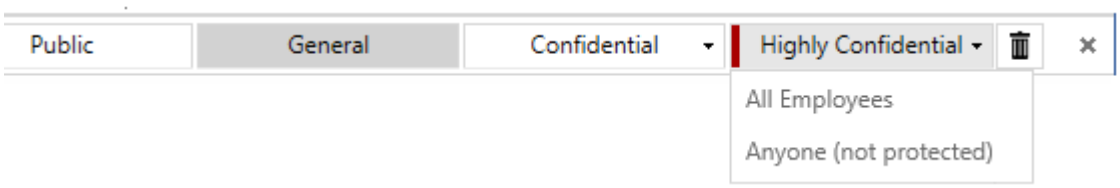
	BYOK with SharePoint	HYOK with SharePoint
Complexity	Complex	Most complex
Encryption technology	Azure Information Protection service	AD RMS on premises
Where protection is defined	Azure Rights Management Templates (in Azure)	AD RMS rights policy template (on premises)
Where classification labels are defined	Azure Information Protection policy (in Azure)	Azure Information Protection policy (in Azure)
Requires user action	Yes	Yes
Works with search, Delve, eDiscovery, co-authoring, and other collaborative features of Office 365	No	No
Requires federated identity integration (such as AD FS)	No	Yes
Requires on-premises components	No	Yes

Configuring protection for BYOK and HYOK solutions

Protection is applied to a file by using the Azure Information Protection client to select a label. See the description for Azure Information Protection classification and labeling earlier in this content.

For these scenarios consider creating a custom sub-label.

The protection that is applied is configured in different places for BYOK and HYOK.



For both BYOK and HYOK solutions:

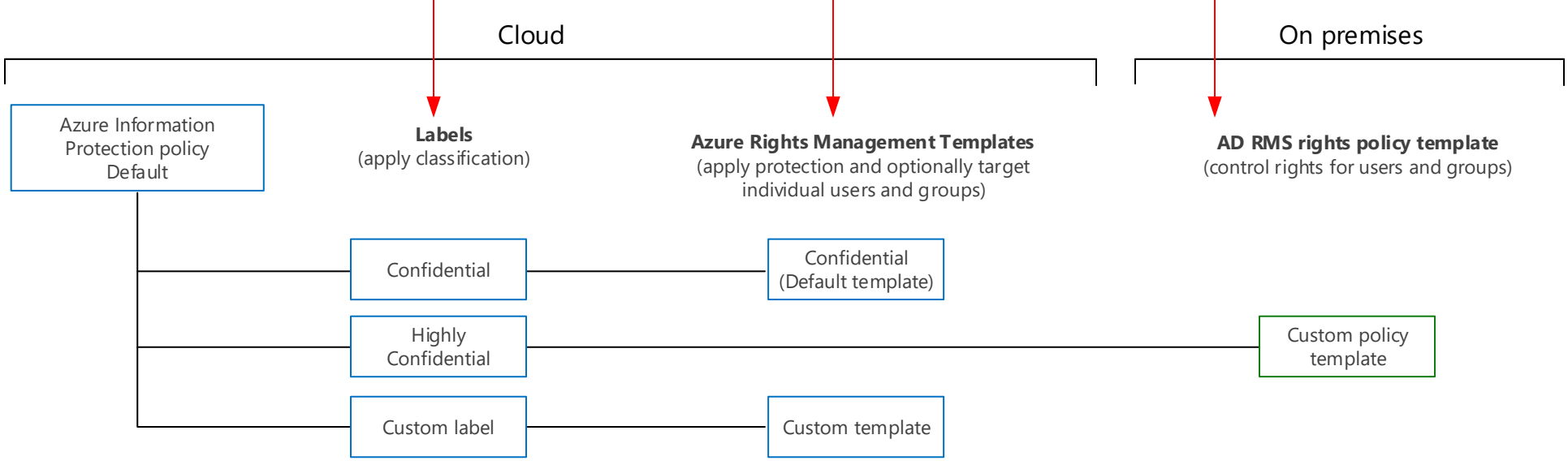
- Review the classification labels and make any changes you need.

For BYOK:

- Modify one of the default Azure Rights Management Templates or create a new template with the desired protection.

For HYOK:

- Create a custom AD RMS rights policy template on-premises for your highly classified or regulated data.



You can customize the default labels and add new labels to the default Azure Information Policy.

The default Azure Information Protection policy

Create a new label for Azure Information Protection

How to configure a label to apply Rights Management protection

You can associate one of the default Azure Rights Management templates to a label. You can also customize the two default Azure Rights Management templates.

You can create new Azure Rights Management templates and apply these to a label.

Create, configure, and publish a custom template

Configure usage rights for Azure Rights Management

For HYOK file protection solutions, create an AD RMS rights policy template for the on-premises AD RMS cluster.

Then, associate the AD RMS protection policy with an Azure Information Protection classification label by copying the AD RMS template GUID and cluster licensing URL into your Azure Information Protection admin portal.

AD RMS Policy Templates

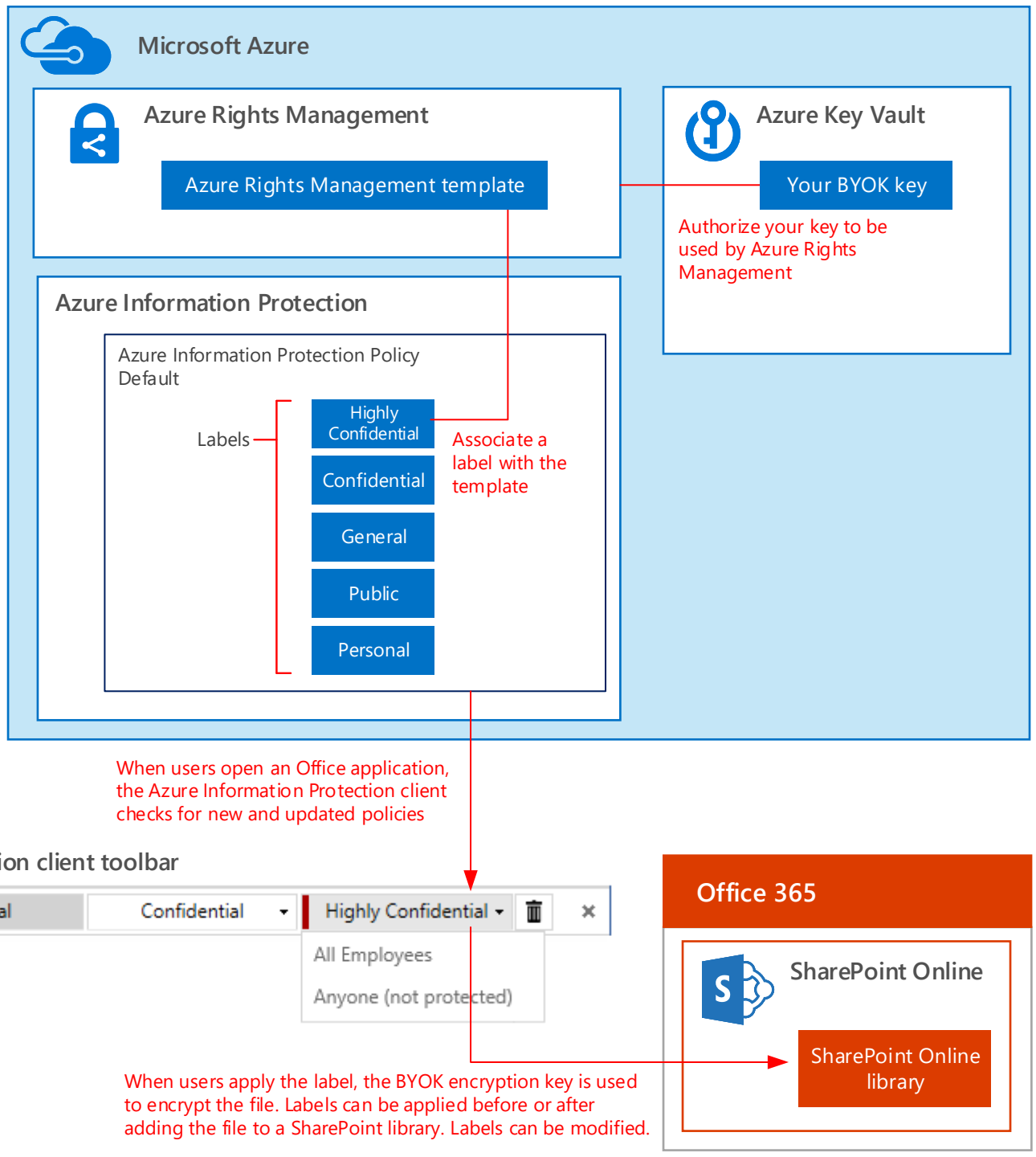
See "Configuring HYOK" in this blog

Continued on next page

Bring Your Own Key (BYOK) with Azure Information Protection and SharePoint Online

This solution is all in the cloud.

- You generate an encryption key based on your requirements and store it in Azure Key Vault.
- You customize or create a new Azure Rights Management template with the protections needed for your data.
- You associate this policy template with a label in the Azure Information policy.
- Users apply protection by using the Azure Information Protection client toolbar to select a label.
- You can use a private Office 365 Group or a Microsoft Teams team to manage permissions to these files, including who can see the library.



Deployment

1 Create your own key vault in Azure

Create a hardened container (a vault) in Azure, to store and manage cryptographic keys and secrets in Azure.

Get started with Azure Key Vault

2 Add your key to the key vault

Generate your own key and transfer it to the Azure Key Vault or create it directly in the vault.

Add a key or secret to the key vault

3 Activate Azure Rights Management

This service might already be activated for your organization.

Activating Azure Rights Management

4 Configure the Azure Rights Management service to use your encryption key

Authorize the Azure Rights Management service to use the key.

Planning and implementing your Azure Information Protection tenant key

5 Decide what classification labels) to apply to your sensitive files

You can customize the default labels and add new labels.

Default Azure Information Protection policy settings

6 Update the labels to support your decisions

Reconfigure the default Azure Information Protection labels to make any changes you need to support your classification decisions.

How to configure a label to apply Rights Management protection

7 Configure Azure Rights Management templates and associate these with labels

Modify one of the default templates or create a new template. Choose the protections to apply to your sensitive data, in addition to encryption.

Create, configure, and publish a custom template

Configure usage rights for Azure Rights Management

8 Create a private Office 365 group or a Microsoft Teams team and add members

You can script and automate the installation, or users can install the client manually.

Create an Office 365 Group in the admin center

Turn on Microsoft Teams

Microsoft Teams Help

9 Install the Information Protection client and train users

You can script and automate the installation, or users can install the client manually.

The client side of Azure Information Protection

Installing the Azure Information Protection client

Continued on next page

Using the solution

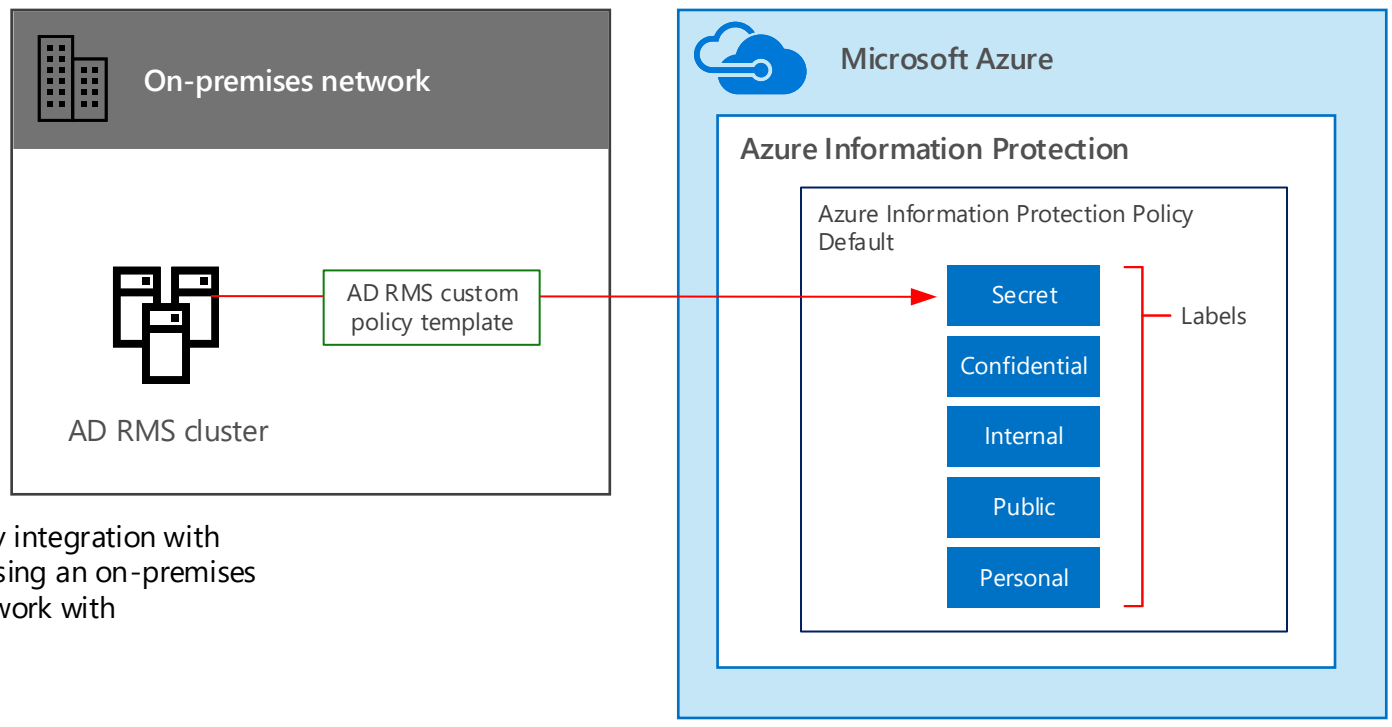
1. **Install the Information Protection client**
   If installation isn't automated, users can install the client manually.
   Download page for manual installation
2. **Use the client toolbar to apply labels**
   HYOK encryption is applied, including additional protections that are configured in the RMS policy template.
3. **Upload files to the SharePoint library**
   Be sure users know which SharePoint library to use for your highly confidential or regulated data. Be sure the SharePoint library is NOT IRM protected.

Hold Your Own Key (HYOK) with RMS and SharePoint Online

This solution brings together components on premises and in the cloud.

- AD RMS uses RMS policy templates to apply protection to files.
- You define a custom RMS policy template for your highly classified or regulated data.
- You associate this policy template with a label in the Azure Information policy.

This solution requires federated identity integration with Office 365 to make use of encryption using an on-premises encryption key. This solution does not work with synchronized identities.



Deployment

1. **Activate Azure Rights Management**
   Azure Information Protection services are always cloud hosted but they enable you to operate in a cloud-only, hybrid, or on-premises only deployment.
   Activating Azure Rights Management
2. **Decide what classification label(s)s to apply to your sensitive files**
   You can customize the default labels and add new labels.
   Default Azure Information Protection policy settings
3. **Update the labels to support your decisions**
   Reconfigure the default Azure Information Protection labels to make any changes you need to support your classification decisions.
   How to configure a label to apply Rights Management protection
4. **Deploy an Active Directory RMS cluster on premises**
   Hold your own key (HYOK) requirements and restrictions for AD RMS protection
   Active Directory Rights Management Services Overview
   Test Lab Guide: Deploying an AD RMS Cluster
5. **Create, configure, and deploy a custom RMS policy template**
   This policy template is part of the on-premises RMS deployment.
   AD RMS Policy Templates
   AD RMS Rights Policy Templates Deployment Step-by-Step Guide
6. **Associate the AD RMS policy template with an Azure Information Protection classification label**
   Copy the AD RMS template GUID and cluster licensing URL into our Azure Information Protection admin portal.
   See "Configuring HYOK" in this blog: Azure Information Protection with HYOK
7. **Create a private Office 365 group or a Microsoft Teams team and add members**
   You can script and automate the installation, or users can install the client manually.
   Create an Office 365 Group in the admin center
   Turn on Microsoft Teams
   Microsoft Teams Help
8. **Get ready to train users**
   Produce user guidance that explains which label to apply and when.
9. **Install the Information Protection client**
   You can script and automate the installation, or users can install the client manually.
   The client side of Azure Information Protection
   Installing the Azure Information Protection client

Using the solution

1. **Install the Information Protection client**
   If installation isn't automated, users can install the client manually.
   Download page for manual installation
2. **Use the client toolbar to apply labels**
   HYOK encryption is applied, including additional protections that are configured in the RMS policy template.
3. **Upload files to the SharePoint library**
   Be sure users know which SharePoint library to use for your highly confidential or regulated data. Be sure the SharePoint library is NOT IRM protected.

Microsoft