Introduction: summary of knowledge

https://docs.microsoft.com/en-us/learn/certifications/exams/sc-900

1. Implement Information Protection (35-40%)
    1.1. Create and manage sensitive information types
        1.1.1. select a sensitive information type based on an organization's requirements
        1.1.2. create and manage custom sensitive information types
        1.1.3. create custom sensitive information types with exact data match
        1.1.4. implement document fingerprinting
        1.1.5. create a keyword dictionary
    1.2. Create and manage trainable classifiers
        1.2.1. identify when to use trainable classifiers
        1.2.2. create a trainable classifier
        1.2.3. verify a trainable classifier is performing properly
        1.2.4. retrain a classifier
    1.3. Implement and manage sensitivity labels
        1.3.1. identify roles and permissions for administering sensitivity labels
        1.3.2. create sensitivity labels
        1.3.3. configure and manage sensitivity label policies
        1.3.4. apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites
        1.3.5. configure and publish automatic labeling policies (excluding MCAS scenarios)
        1.3.6. monitor data classification and label usage by using label analytics tools such as content explorer and activity explorer
        1.3.7. explorer and activity explorer
        1.3.8. apply bulk classification to on-premises data by using the AIP unified labelling scanner
        1.3.9. manage protection settings and marking for applied sensitivity labels
        1.3.10. apply protections and restrictions to email including content marking, usage, permission,
        1.3.11. encryption, expiration, etc.
        1.3.12. apply protections and restrictions to files including content marking, usage, permission,
        1.3.13. encryption, expiration, etc.
    1.4. Plan and implement encryption for email messages
        1.4.1. define requirements for implementing Office 365 Message Encryption
        1.4.2. implement Office 365 Advanced Message Encryption

2. Implement Data Loss Prevention (30-35%)
    2.1.1. Create and configure data loss prevention policies
    2.1.2. recommend a data loss prevention solution for an organization
    2.1.3. configure data loss prevention for policy precedence
    2.1.4. configure policies for Microsoft Exchange email
    2.1.5. configure policies for Microsoft SharePoint sites
    2.1.6. configure policies for Microsoft OneDrive accounts
    2.1.7. configure policies for Microsoft Teams chat and channel messages
    2.1.8. integrate Microsoft Cloud App Security (MCAS) with Microsoft Information Protection
    2.1.9. configure policies in Microsoft Cloud App Security (MCAS)
    2.1.10. implement data loss prevention policies in test mode
  2.2. Implement and monitor Microsoft Endpoint data loss prevention
    2.2.1. configure policies for endpoints
    2.2.2. configure Endpoint data loss prevention settings
    2.2.3. recommend configurations that enable devices for Endpoint data loss prevention policies
    2.2.4. monitor endpoint activities
  2.3. Manage and monitor data loss prevention policies and activities
    2.3.1. manage and respond to data loss prevention policy violations
    2.3.2. review and analyze data loss prevention reports
    2.3.3. manage permissions for data loss prevention reports
    2.3.4. manage data loss prevention violations in Microsoft Cloud App Security (MCAS)

3. Implement Information Governance (25-30%)
  3.1. Configure retention policies and labels
    3.1.1. create and apply retention labels
    3.1.2. create and apply retention label policies
    3.1.3. configure and publish auto-apply label policies
  3.2. Manage data retention in Microsoft 365
    3.2.1. create and apply retention policies in Microsoft SharePoint and OneDrive
    3.2.2. create and apply retention policies in Microsoft Teams
    3.2.3. recover content in Microsoft Teams, SharePoint, and OneDrive
    3.2.4. recover content in Microsoft Exchange
    3.2.5. implement retention policies and tags in Microsoft Exchange
    3.2.6. apply mailbox holds in Microsoft Exchange
    3.2.7. implement Microsoft Exchange Online archiving policies
  3.3. Implement records management in Microsoft 365

3.3.1. configure labels for records management
3.3.2. manage and migrate retention requirements with a file plan
3.3.3. configure automatic retention using File Plan descriptors
3.3.4. classify records using retention labels and policies
3.3.5. implement in-place records management in Microsoft SharePoint
3.3.6. configure event-based retention
3.3.7. manage disposition of records

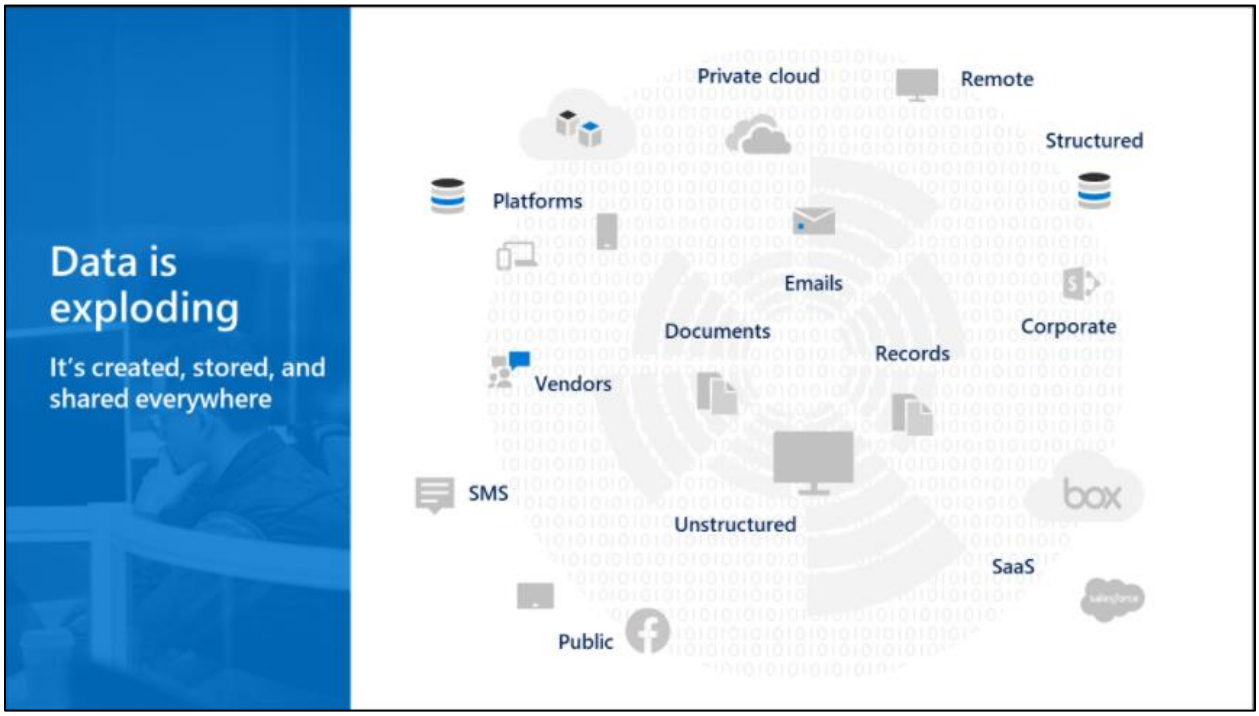
1. Implement Information Protection

1.1. Introduction to information protection and governance in Microsoft 365

1.1.1. Introduction to information and governance in Microsoft 365

1.1.1.1. Data is exploding

Data is exploding and it is being created, stored, and shared everywhere. IDC estimates that in 2025, the world will create and replicate 163 zettabytes of data, representing a tenfold increase from the amount of data created in 2016. Not only is the amount of data growing, but the types of data continue to evolve. In the past, organizations primarily dealt with documents and emails. Now they are also dealing with instant messages, text messages, video files, and images. Many organizations are struggling with how to manage this data overload and the variety of devices on which it is created.



1.1.1.2. Regulation is increasing

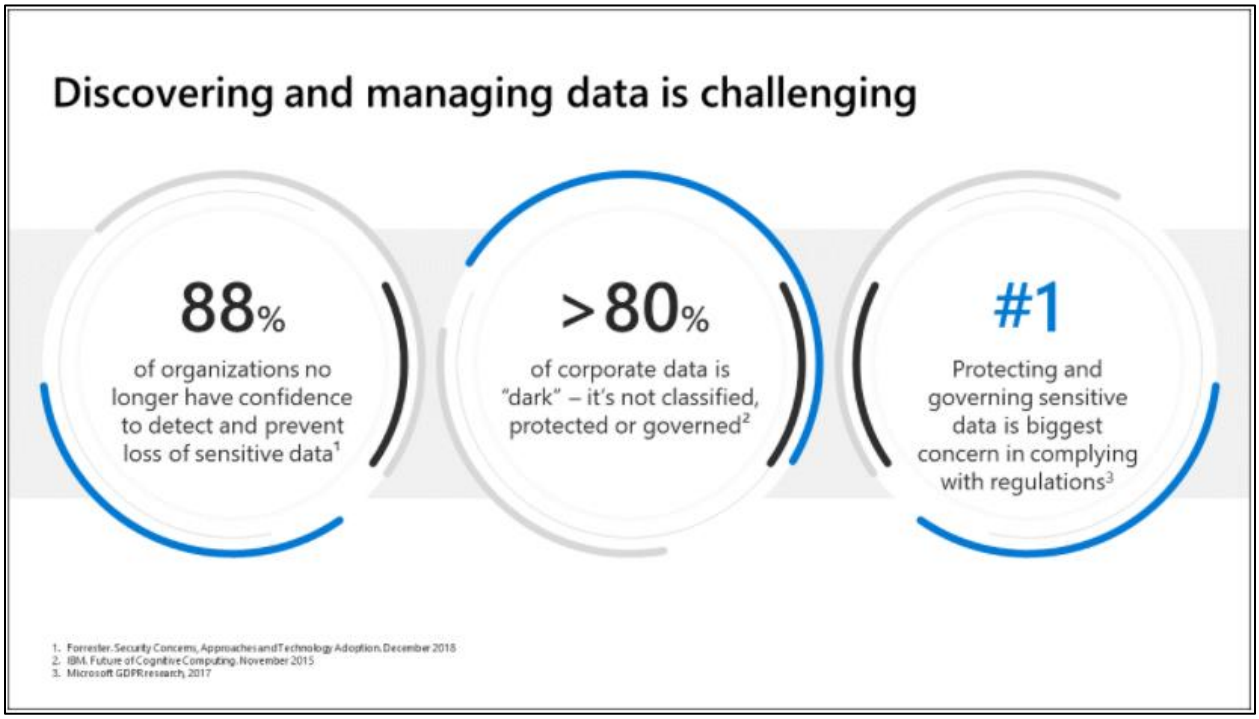
Not only is the amount of data increasing, the number of regulations organizations must comply with continues to grow. The maintenance and protection of personal data is one area where there has been a lot of focus. The cost of not complying with privacy regulations like the European General Data Protection Regulation (GDPR) could result in fines, withdrawal of licenses, and lower credibility with regulators and customers.

1.1.1.3. Discovering and managing data is challenging

Many organizations are struggling with managing their data. Research tells us most organizations do not have the information to understand the risks they face. Protecting data has become more challenging as people work in new ways, including creating and sharing data across organizational, or regional boundaries. Customers now need to protect sensitive information on devices, Software as a Service (SaaS) applications, and cloud services, in addition to on-premises environments. Your risk profile is likely to increase without an information protection and governance strategy. Here are few points to consider:

- 88% of organizations no longer have the confidence they can detect sensitive data loss or protect against it.
- More than 80% of corporate data is "dark", meaning it is not classified, protected, or governed.

- Protecting and governing sensitive data is the biggest concern in complying with regulations.



1.1.1.4. Defining an information and protection strategy

Does your organization have a strategy to detect, manage and protect sensitive information across your digital estate? One of the first questions our customers ask when discussing information protection and governance goes something like this: "How can I implement a strategy for protecting and managing sensitive information?"

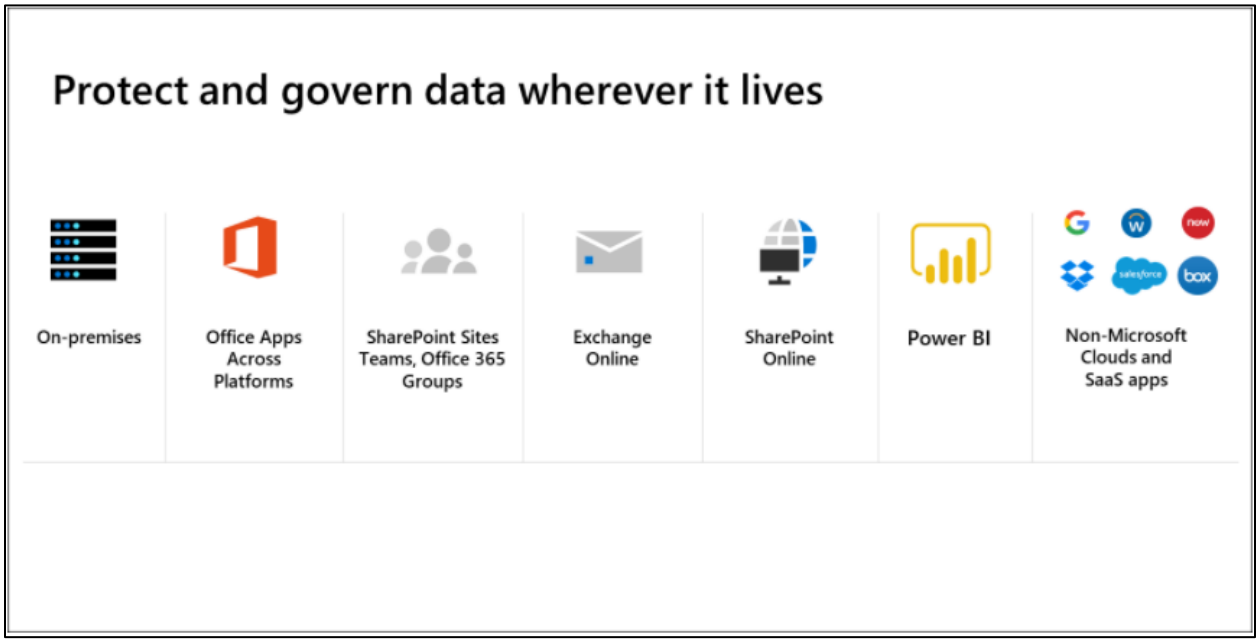
Here are some common questions we ask when talking with our customers about this topic:

- *Do you know where your business critical and sensitive data resides and what is being done with it?* Trying to understand where your information is can be a huge project in itself.
- *Do you have control of this data as it travels inside and outside your organization; for example, when it gets shared with customers or partners via email, SharePoint sites, or other online services, or is copied to a mobile device?* You want to protect information wherever it goes.
- *Are you using multiple solutions to classify, label, and protect sensitive data?* We find that many organizations use more than one solution to protect and govern their data, making it difficult to determine if there are any coverage gaps.

1.1.1.5. Protect and govern data wherever it lives

Microsoft offers integrated information protection and governance solutions to help you protect and govern your data, throughout its lifecycle – wherever it lives, or wherever it travels.

It is not just about the data in Microsoft 365 services like Exchange Online, SharePoint Online and Microsoft Teams. You probably have data in other locations like on-premises SharePoint sites and local file shares. Sensitive data also resides in data visualization tools, like Power BI. Your organization might also use non-Microsoft clouds like Dropbox, Box, or software-as-a-service (SaaS) apps like Salesforce. And let's not forget about your corporate social networking presence. The image below lists some possible sensitive data storage locations.



1.1.1.6. Unified approach to data discovery and classification

Microsoft is taking a unified approach to the discovery and classification of data in Microsoft 365 services, our productivity apps, the Power Platform, non-Microsoft cloud services and apps, and on-premises data. The benefits of this approach include:

- Consistent classification across devices, apps, and services.
- Strong integration into the applications and services.
- Deep content scanning with more than 90 built-in sensitive information types.
- Fully extensible scanning with support for custom sensitive information types and trainable classifiers.

1.1.1.7. Balance security and productivity

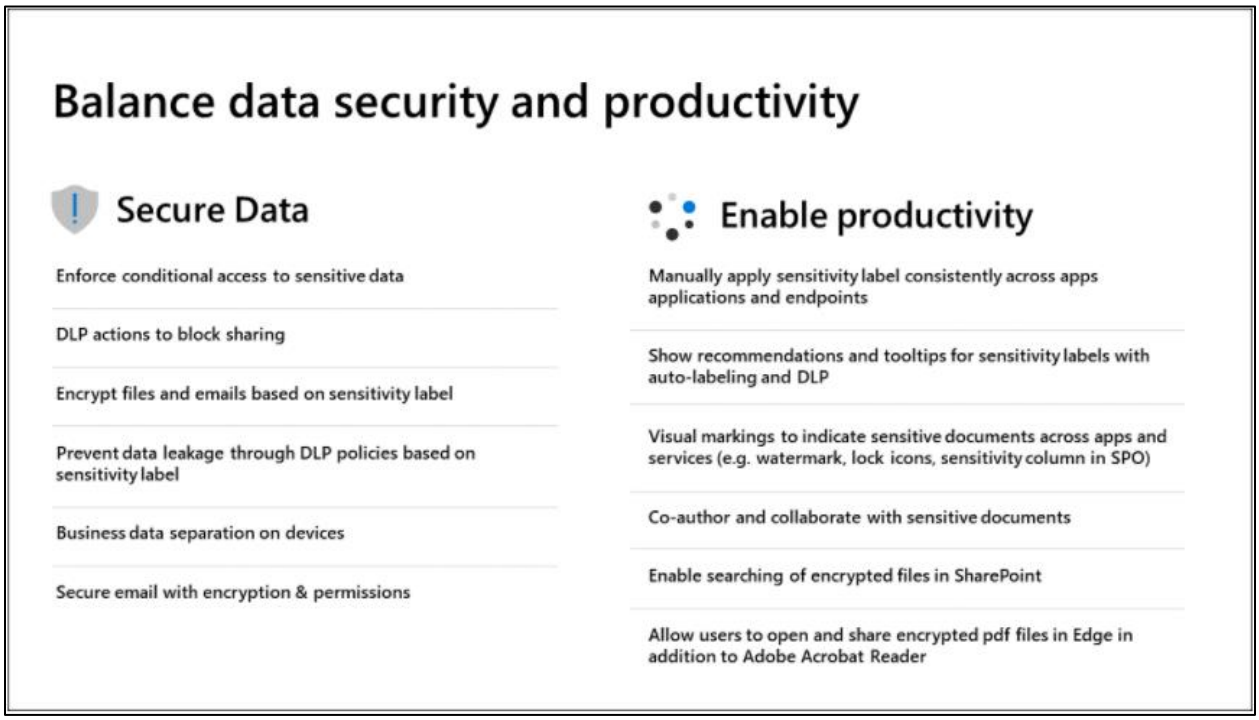
You must strike a balance in the organization's interest in security with your workforce's desire for mobility and productivity.

These capabilities tip the security side of the scale:

- Enforce Conditional Access to sensitive data.
- Data loss prevention (DLP) actions to block sharing.
- File and email encryption based on sensitivity label.
- Prevent data leakage through DLP policies.
- Business data separation on devices.
- Secure email with encryption and permissions.

These capabilities tip the productivity side of the scale:

- Seamless built-in experiences across Office apps on all platforms.
- Flexible search, collaboration, and co-authoring on protected files in Office on the Web.
- Recommended labeling and visual markings like watermarks, lock icons, and policy tips.
- Built-in labeling in Office applications on iOS and Android.



1.1.1.8. Information protection and governance lifecycle

Implementing an information and governance solution for your organization is a journey, and every organization will take a different approach. Whatever approach you use, it will involve people, processes, and technology.

1.1.1.8.1. People

The information protection governance lifecycle involves many potential stakeholders. In your organization, there may not be people with the specific titles listed below. The important thing to remember is that each of these roles should be represented:

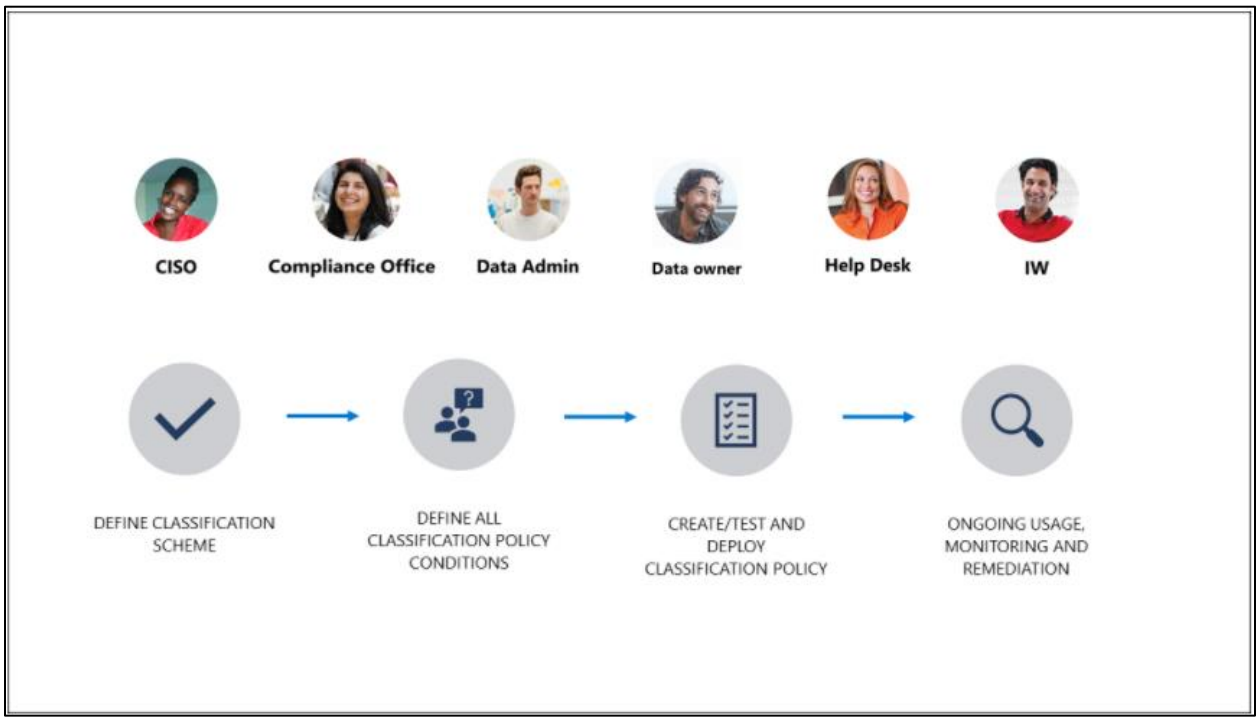
- **Chief Information Security Officer (CISO)**. Typically head of the governance committee. Determines policies and procedures.
- **Compliance Officer**. Understands and interprets regulations, which ones apply to the organization, and what kind of controls are needed.
- **Data Admin**. Writes sensitive information classification policies based on guidance provided by the governance committee.
- **Data Owner**. Business owner of the content or process.
- **Help Desk**. Trained on how to assist information workers when issues arise; for example, when access to a document is lost for an unknown reason.
- **Information Worker**. Creates documents, emails, or other content that may be affected by policies and procedures. They need to know what classification means, when it should be applied, what happens if it is auto-applied, etc. Information workers are referred to as users in this learning path.

1.1.1.8.2. Process

From a process perspective, here are the major phases you should follow for a successful implementation.

- **Define the data classification taxonomy**. The data classification taxonomy ends up as sensitivity and retention labels that will be applied to your content. These labels may surface in productivity applications, SharePoint Online sites, Microsoft Teams workspaces and Exchange emails. They may be applied manually by users or automatically by Microsoft 365.
- **Define classification policy conditions**. Once you have built your taxonomy, you need to determine how you are going to find and classify the data in your environment and map it to the taxonomy.

- **Create, test, and deploy the labels and policy settings**. Once you determine the methods you will use to protect and govern your data, it is important to test everything thoroughly prior to deploying your configuration across the organization.
- **Ongoing usage, monitoring and remediation**. It is important to understand how data classification is being used and to ensure your policies are accurate and achieving the desired results.



1.1.1.8.3. Technology

Lastly, you need a technology partner with the right solutions to meet your needs. In this course we will explore the unique capabilities Microsoft delivers to meet your data classification, information protection, and information governance requirements.

1.1.1.9. Know your data, protect your data, prevent data loss, and govern your data

Microsoft's approach to information protection and governance is centered around four principles:

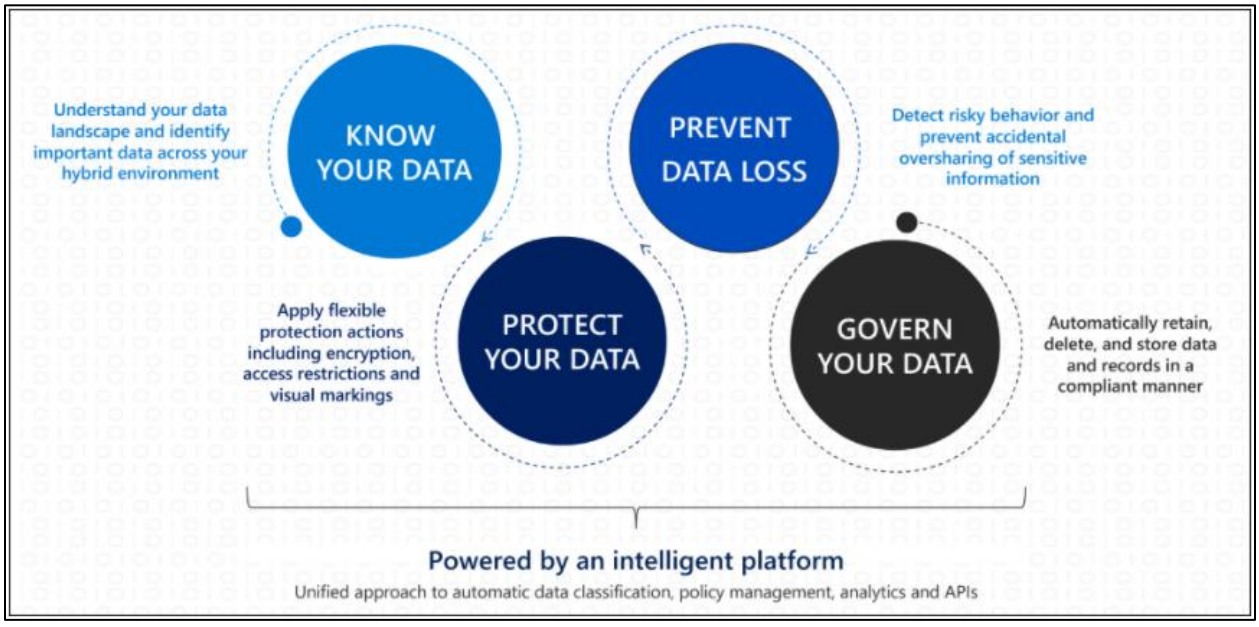
- *Know your data*. Understand your data landscape and identify important data across your hybrid environment.
- *Protect your data*. Apply flexible protection actions including encryption, access restrictions, and visual markings.

- *Prevent data loss*. Detect risky behavior and prevent accidental oversharing of sensitive information.
- *Govern your data*. Automatically retain, delete, and store data and records in a compliant manner.

Knowing your data, protecting your data, preventing data loss, and governing your data are outcomes powered and enriched by our intelligent platform, which delivers:

- A common approach to classification, no matter where data resides.
- A unified policy configuration and management experience for Information Technology (IT).
- An analytics dashboard to monitor and remediate issues.
- Application Programming Interfaces (APIs) that enable the partner ecosystem to extend information protection and governance capabilities to their own apps and services.

As the image below illustrates, information protection and governance is not something you do once and then you are finished. It is a continuous process where you start with the basics and refine your approach over time.



1.1.2. Know your data

The first challenge many organizations face is identifying what kind of, and how much, data exists in their environment. You need a deep understanding of how much sensitive data exists and where it is stored before it can be protected and governed. This

information is critical to assess your overall risk, which helps you define your strategy for protecting and governing the data. Start your journey by discovering and classifying important data across your environment. Here are some of the types of questions you will answer during this process:

1. Who owns my data?
2. What types of data do I have?
3. Where is my data?
4. Why is it a risk?
5. What methods can I use to classify my data?
6. Where can I classify my data?
7. How can I see what happens to my data over its lifecycle?

1.1.2.1. Data classification concepts

Classification is the process of identifying and labeling content in your organization to get a better understanding of your data landscape. This is accomplished by applying one or more of the following to your data:

- Sensitive information types
- Trainable classifiers
- Labels
- Policies

1.1.2.1.1. Sensitive information types

Most information protection and governance workflows leverage sensitive information types. A sensitive information type is defined by a pattern that can be identified by a regular expression or function. One commonly recognized sensitive information type is a credit card number. Microsoft includes about 100 of the most common sensitive information types, or you can create your own.

1.1.2.1.2. Trainable classifiers (currently in preview)

Data can also be classified via trainable classifiers. Trainable classifiers use artificial intelligence and machine learning to intelligently classify your data. They are most useful classifying data unique to an organization like specific kinds of contracts, invoices, or customer records. This method of classification is more about training a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching).

1.1.2.1.3. Labels

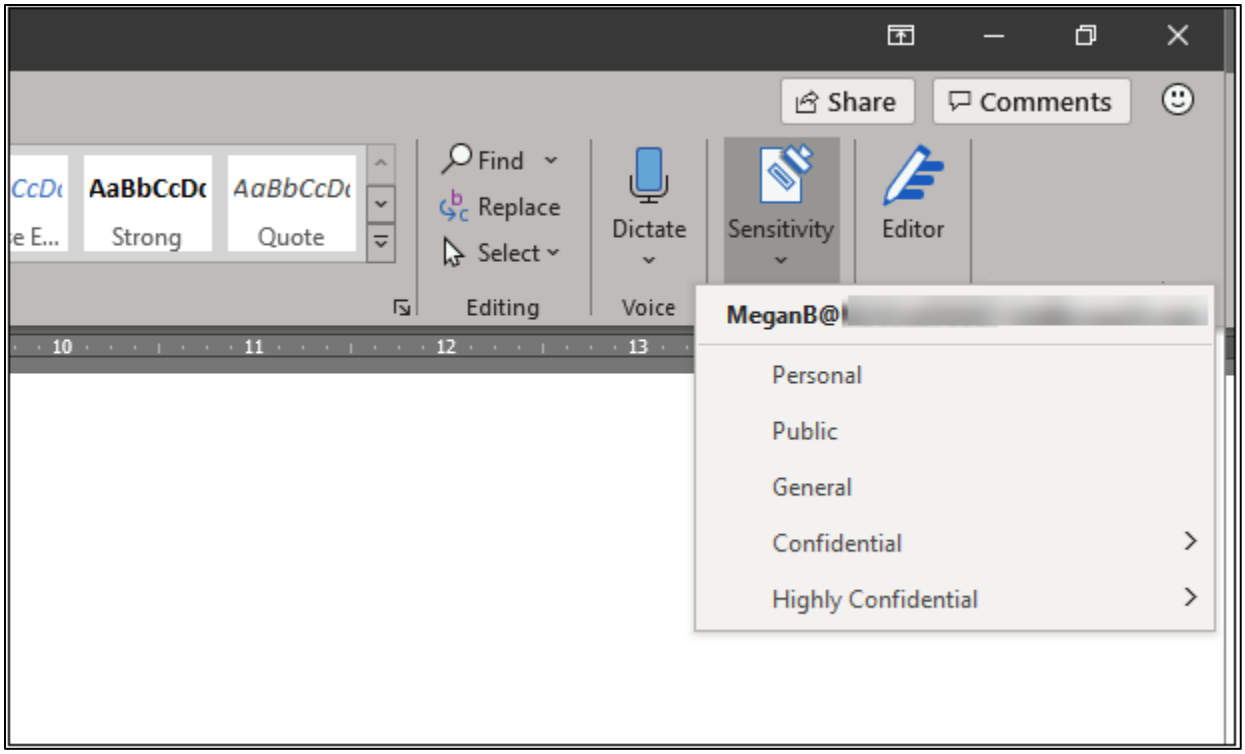
A label can be thought of as a stamp on a document. For example, your organization might create a label named "Confidential" to indicate data that should not be widely shared or that it should be retained for a specific time period. Labels can, but do not have to, use sensitive information types to classify email messages, documents, sites, and more. Microsoft information protection and governance solutions use two forms of labels, sensitivity labels and retention labels. You can prevent users from changing labels by applying encryption to the content.

With sensitivity labels, you can classify and help protect your sensitive content. Protection options include adding watermarks or encryption to the content. Sensitivity labels persist wherever your document is stored or sent.

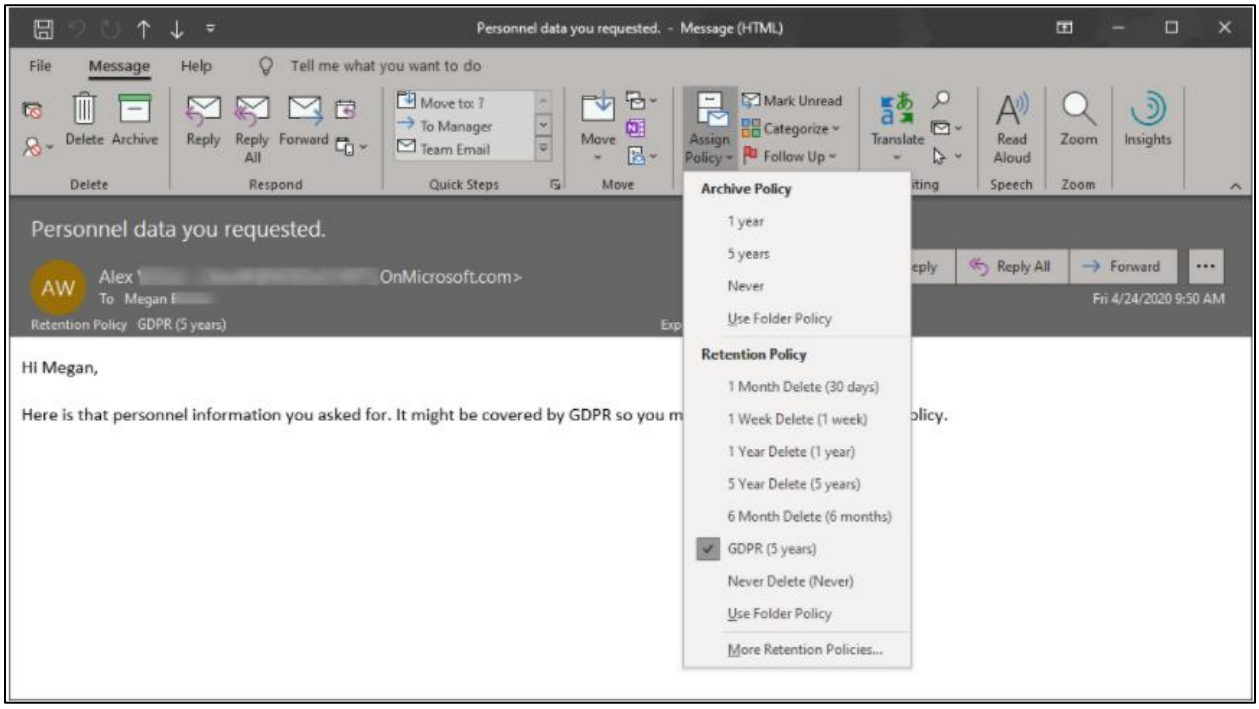
Retention labels help you retain or delete content based on policies you define. These help organizations comply with industry regulations and internal policies. Retention labels do not persist outside Microsoft 365.

Unlike retention labels, which are published to locations such as all Exchange mailboxes, sensitivity labels are published to users or groups. Sensitivity labels then appear in Office apps for those users and groups.

This image shows how you select a sensitivity label in a Word document.



This image shows a retention label named GDPR applied to an email in Outlook.



Content can have both a sensitivity label and a retention label associated with it, but not more than one of each. An example might be an Excel file with a sensitivity label of "Internal use only" and a retention label named "Employee Record".

1.1.2.1.4. Policies

Once classified, you can create policies. Sensitive information types, trainable classifiers, sensitivity labels, and retention labels act as inputs into policies. Policies define behaviors, like if there will be a default label, if labeling is mandatory, what locations the label will be applied to, and under what conditions. A policy is created when you configure Microsoft 365 to publish or automatically apply sensitive information types, trainable classifiers, or labels.

Sensitivity label policies show one or more labels to Office apps (like Outlook and Word), SharePoint sites, and Office 365 groups. Once published, users can apply the labels to protect their content.

Data loss prevention (DLP) policies help identify and protect your organization's sensitive info. For example, you can set up policies to help make sure information in email and documents is not shared with the wrong people. DLP policies can use sensitive information types and retention labels to identify content containing information that might need protection.

Retention policies and retention label policies help you keep what you want and get rid of what you do not. They also play a significant role in records management.

1.1.2.2. Classify data directly in Office apps

Microsoft makes the process of classifying, labeling, and protecting content a consistent and easy experience for users. Users apply and update labels while working in Word, PowerPoint, Excel, and Outlook. With built-in labeling, sensitivity labeling capability is integrated natively into Office apps. No plug-ins or add-ons are required for most users running the latest Office releases. The same labels and policies apply across Office on Mac, iOS, Android, Windows, and web.

1.1.2.2.1. Manual labeling on all platforms

Built-in manual labeling is available on all Office app platforms. Windows users must be running Microsoft 365 Apps for enterprise (formerly known as Office 365 ProPlus) version 1910 or later, or an add-on will still be required. A Microsoft 365 Apps for enterprise subscription is also required for macOS users.

1.1.2.2.2. Automated labeling in Office for the web and Windows

The capability for users to do manual labeling is certainly a step in the right direction, but users cannot always be relied upon to do this on their own. Automated labeling is available in Office apps starting with Office on the web and Office on Windows. Users can override the automatically applied labels provided the administrator has configured the system to allow it.

1.1.2.2.3. Automated labeling on content stored in OneDrive, SharePoint, and Exchange

You can now create auto-labeling policies to automatically apply sensitivity labels to email messages or documents stored in Microsoft 365 services like OneDrive, SharePoint, and Exchange. Because this labeling is applied by services rather than by applications, you do not need to worry about what apps users have and what version they are using.

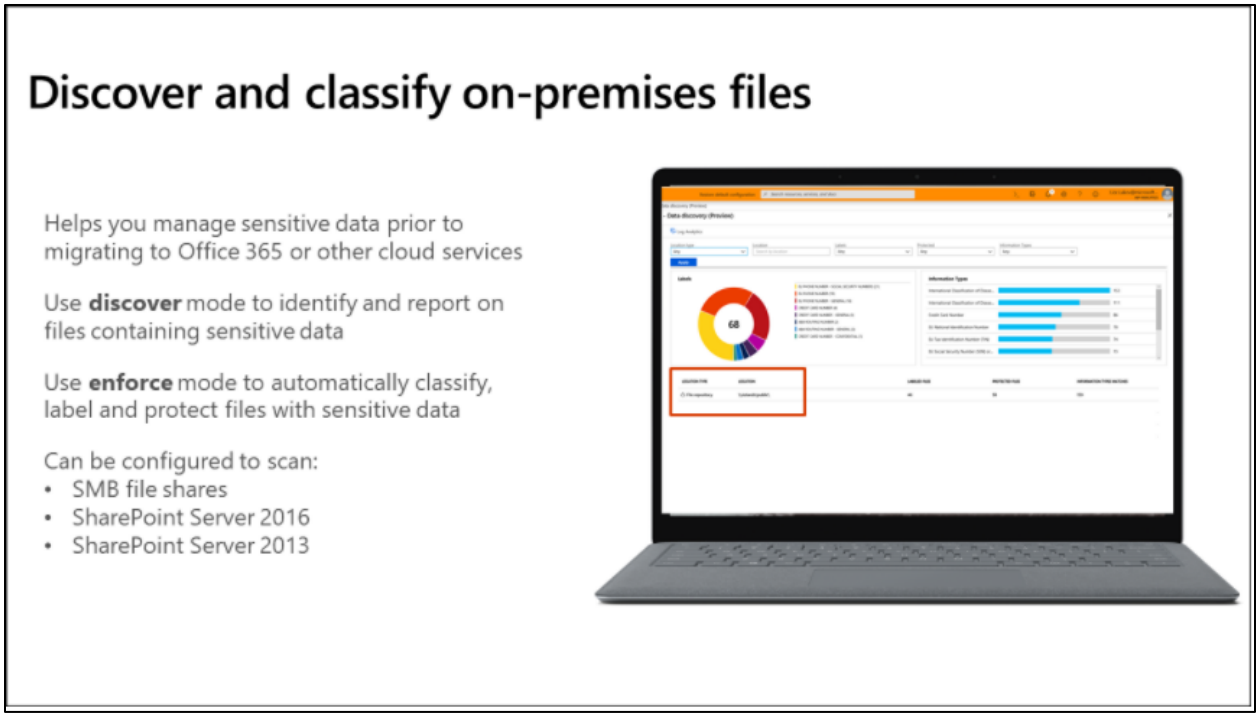
1.1.2.3. Discover and classify Microsoft 365 content

The ability to discover and classify data in Microsoft 365 apps and services is part of the core functionality of Microsoft's information protection and governance solutions. These locations include the following:

- Exchange email
- SharePoint sites
- OneDrive accounts
- Teams messages and chats

1.1.2.4. Discover and classify on-premises files

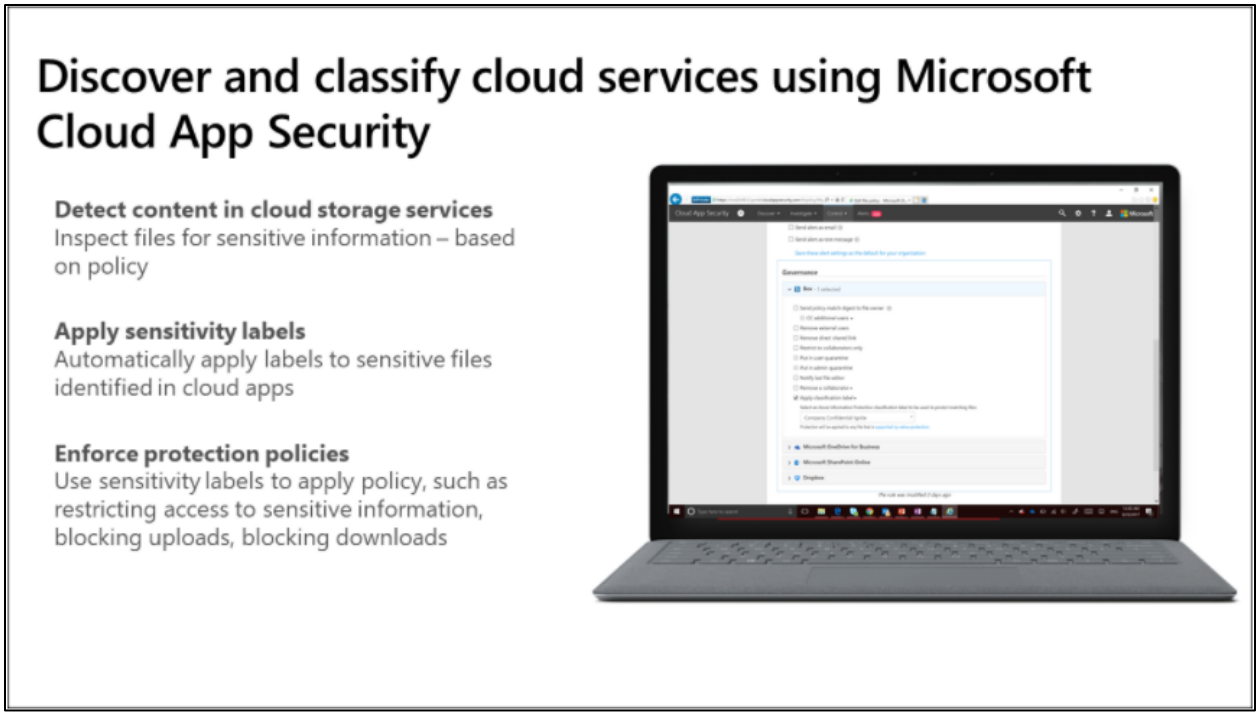
Azure Information Protection scanner helps discover, classify, label, and protect sensitive information in on-premises file servers. You can run the scanner and get immediate insight into risks with on-premises data. Discover mode helps you identify and report on files containing sensitive data. Enforce mode automatically classifies, labels, and protects files with sensitive data.



1.1.2.5. Discover and classify cloud services and SaaS apps

Most organizations store some of their sensitive data outside the Microsoft ecosystem. Microsoft Cloud App Security extends protection to third-party clouds and SaaS applications. This solution includes the following capabilities:

- Inspect files for sensitive information
- Automatically apply labels to sensitive files identified in cloud apps
- Use sensitivity labels to apply policy, such as restricting access to sensitive information, blocking uploads, and blocking downloads



1.1.3. Protect your data

Customers typically want to apply some level of protection to the most sensitive data to prevent it from getting into the wrong hands. Microsoft's solution for meeting this requirement is *information protection*. It helps you discover, classify, and protect sensitive and business-critical content across your organization. This is accomplished by enabling users and admins to apply flexible protection actions, from applying visual markings to adding encryption and access restrictions to content.

Not all data is created equal. You need the flexibility to apply a different level of protection to a highly confidential file that contains company financial data versus a file that contains information on the company picnic. Information protection is covered in more depth in other modules in this learning path, but here are some key themes of the Microsoft solution for protecting your data.

1.1.3.1. Built-in experiences

Information protection is integrated into Microsoft 365 apps like Word and Excel, Microsoft 365 services like SharePoint Online and Microsoft Teams, other Microsoft solutions like Power BI.

1.1.3.2. Broad coverage

It is not just about protecting content stored in Microsoft 365. Sensitive information can be protected on devices, on-premises file repositories, and third party cloud services.

1.1.3.3. Flexible labeling options

You can choose between automatic labeling, manual user-driven labeling, or recommended labeling. With flexible labeling options, you can meet your security requirements without impacting end-user productivity.

1.1.4. Prevent data loss

Organizations must protect sensitive information and prevent its inadvertent disclosure to comply with business requirements and industry regulations. End users do not always know what information they are permitted to share with others in and outside the organization. They may also share sensitive data accidentally. The data loss prevention (DLP) solution detects sensitive content and helps prevent accidental oversharing in and outside the organization. How you handle detected sensitive can be influenced by:

1.1.4.1. Data source

The source of the data sharing activity may impact your response. Some users, like members of a finance department, might have a business need to share taxpayer information numbers, while members of a marketing department do not.

1.1.4.2. Data destination

You can adjust your response based on if the sensitive information is shared with people inside your organization, outside your organization, or both.

1.1.4.3. Amount shared

You may determine a user sharing a single credit card number is not as serious as a user sharing 1000 credit card numbers. DLP allows you to respond differently to an oversharing incident based on the amount of data being shared.

1.1.4.4. Exposure impact

You might do something as simple as prompt the user with a tool tip to educate them about sensitive data sharing when the impact of exposing that data is relatively low. Sharing of more sensitive information might result in an incident report being sent to

administrators. Sharing of the most sensitive data could result in blocking content sharing and the content being encrypted.

1.1.5. Govern your data

Governing your data is about keeping what you need and deleting what you don't, to meet compliance requirements and reduce your overall risk landscape. Microsoft's solutions for governing your data are Information governance and Records management.

Information governance manages your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you do not.

Records management uses intelligent classification to automate and simplify the retention schedule for regulatory, legal, and business-critical records in your organization. It is for that special set of content that needs to be immutable (cannot be changed).

Information governance and **Records management** are covered in more depth in other modules in this learning path, but here are some key themes of the Microsoft solutions for governing your data.

1.1.5.1. Streamlined administration

Centralized policy administration allows you to incorporate data inside and outside Microsoft 365 to be managed by the same set of policies. You can create one policy and have it apply across multiple services.

1.1.5.2. Automation at scale

Governance policies can be configured to work automatically and applied organization-wide, if desired. For example, the system can be configured to delete obsolete or irrelevant data without user intervention, reducing the amount of data to govern.

1.1.5.3. Tailored workflows

Retention policies are flexible including the capability to create custom events, such as the departure of an employee, to trigger the retention process. Disposition review lets you name specific people, per label, to review and determine what should be done for each item reaching the end of its retention period.

1.1.6. Summary and knowledge check

The exponential growth of data, blurring of traditional organizational boundaries, and increased workforce collaboration, has made protecting and governing important data more challenging than ever. Data is created, stored, and shared across many locations – devices, apps, cloud services and on-premises. The evolving compliance landscape only adds to the complexity.

Microsoft's comprehensive solutions enable you to protect and govern your data, throughout its lifecycle – wherever it lives, or wherever it travels. We give customers the flexibility to implement the necessary controls to meet both internal and external security and compliance requirements.

Now that you have completed this module, you should be able to:

- Discuss information protection and governance and why it's important.
- Describe Microsoft's approach to information protection and governance.
- Define key terms associated with Microsoft's information protection and governance solutions.
- Identify the solutions that comprise information and governance in Microsoft 365.

1.1.6.1.1. Check your knowledge

1.1.6.1.1.1. Question

1. Which of the following define what to do with data that has been classified?

- Sensitive information types
- Labels
- Policies

1.1.6.1.1.1.1. Correct Answer

Policies define what to do with the data to which has been classified. For example, you can create a policy based on the ***Confidential*** sensitivity label. That label policy can do nothing more than mark a file as confidential, or it can encrypt files, add content marking, and control user access to specific sites based on that sensitivity label.

1.1.6.1.1.1.2. Wrong Answer

- Sensitive information types

A sensitive information type is defined by a pattern that can be identified by a regular expression or function. One commonly recognized sensitive information type is a credit card number.

- Labels

Labels can be thought of as a stamp you put on a document that goes everywhere the document goes, across apps, devices, and services. For example, your organization might create a label named ***Confidential*** to indicate data that should not be widely.

1.1.6.1.1.2. Question

2. Governing your data is all about reducing risk. Which of the following Microsoft solutions for protecting your data is focused on controlling the data explosion, the amount of data being generated and how regulations keep changing?

- Automation at scale
- Streamlined administration
- Records management

1.1.6.1.1.2.1. Correct Answer

- Automation at scale

Automation is scale is all about controlling that data explosion we have been talking about and it's about scaling and automating.

1.1.6.1.1.2.2. Wrong Answer

- Streamlined administration

Managing a set of governance policies in SharePoint, another set in Exchange, and then another for each of your line of business systems is not productive and can be redundant. Microsoft centralized the administration of policies in the Microsoft 365 compliance center and added native connectors to let you incorporate data outside Microsoft 365 to be governed by one set of policies

- Records management

Records management is for that special set of content within your organization, which needs to be immutable.

1.1.6.1.1.3. Question

3. Information protection and governance is a dynamic process. It is continuous. If you are at the stage where the organization is asking why this particular data is a risk, which stage are you in the process?

- Know your data
- Protect your data
- Govern your data

1.1.6.1.1.3.1. Correct Answer

You need a deep understanding of how much sensitive data exists and where it is stored before it can be protected and governed. This information is critical to assess your overall risk, which, helps you define your strategy for protecting and governing the data.

1.1.6.1.1.3.2. Wrong Answer

- Protect your data

Once you know your data and mapped your data estate, you can take steps to protect it.

- Govern your data

Governing your data is about keeping what you need and deleting what you don't, to meet compliance requirements and reduce your overall risk landscape.

1.1.6.1.1.4. Question

4. Once you know your data and mapped your data estate, you can take steps to protect it. Which solution helps you discover, classify, and protect sensitive critical content throughout its lifecycle across your organizations?

- Microsoft data loss prevention solution
- Microsoft information governance
- Microsoft information protection solution

1.1.6.1.1.4.1. Correct Answer

Customers typically want to apply some level of protection to the most sensitive information to prevent it from getting into the wrong hands. This solution helps you discover, classify, and protect sensitive and business critical content throughout its lifecycle across your organization.

1.1.6.1.1.4.2. Wrong Answer

- Microsoft data loss prevention solution

The Microsoft data loss prevention solution detects sensitive content as it is used and shared throughout your organization, in the cloud and on devices, and helps prevent accidental data loss.

- Microsoft information governance

Information governance manages your content lifecycle using solution to import, store, and classify business critical data. Governance policies can be configured to work automatically and applied organization-wide, if desired. For example, the system can be configured to delete obsolete or irrelevant data without user intervention, reducing the amount of data to govern.

1.1.6.1.1.5. Question

5. Governing your data is about keeping what you need and deleting what you do not. Which solution uses intelligent classification to automate and simplify the retention schedule for regulatory, legal, and business critical records in your organization?

- Microsoft information governance
- Microsoft records management
- Microsoft information protection solution

1.1.6.1.1.5.1. Correct Answer

- Microsoft records management

Records management uses intelligent classification to automate and simplify the retention schedule for regulatory, legal, and business critical records in your organization. Governance policies can be configured to work automatically and applied organization-wide, if desired. For example, the system can be configured

to delete obsolete or irrelevant data without user intervention, reducing the amount of data to govern.

1.1.6.1.1.5.2. Wrong Answer

- Microsoft information governance

Information governance manages your content lifecycle using solution to import, store, and classify business critical data. Governance policies can be configured to work automatically and applied organization-wide, if desired. For example, the system can be configured to delete obsolete or irrelevant data without user intervention, reducing the amount of data to govern.

- Microsoft information protection solution

Customers typically want to apply some level of protection to the most sensitive information to prevent it from getting into the wrong hands. This solution helps you discover, classify, and protect sensitive and business critical content throughout its lifecycle across your organization. Question: Once you know your data and mapped your data estate, you can take steps to protect it. Which solution helps you discover, classify, and protect sensitive and business critical content throughout its lifecycle across your organization?

1.2.Prevent data loss

1.2.1. Introduction to Microsoft 365 data loss prevention

Data loss prevention (DLP) is an important issue for organization message systems because of the extensive sharing of sensitive information in business-critical communication. To enforce compliance requirements for sensitive data without hindering user productivity, you can use Microsoft 365 DLP features to help protect and manage sensitive data.

This module describes data loss prevention features that can help you identify and monitor sensitive information categories that you have defined within your policies. These features help you create or change DLP policies. You can include rules that include checks for sensitive information such as private identification numbers or credit card numbers. You can also create custom conditions within a policy, such as how many times something has to be found before an action is taken or exactly what that action is.

1.2.2. Define the sensitive data you want to protect

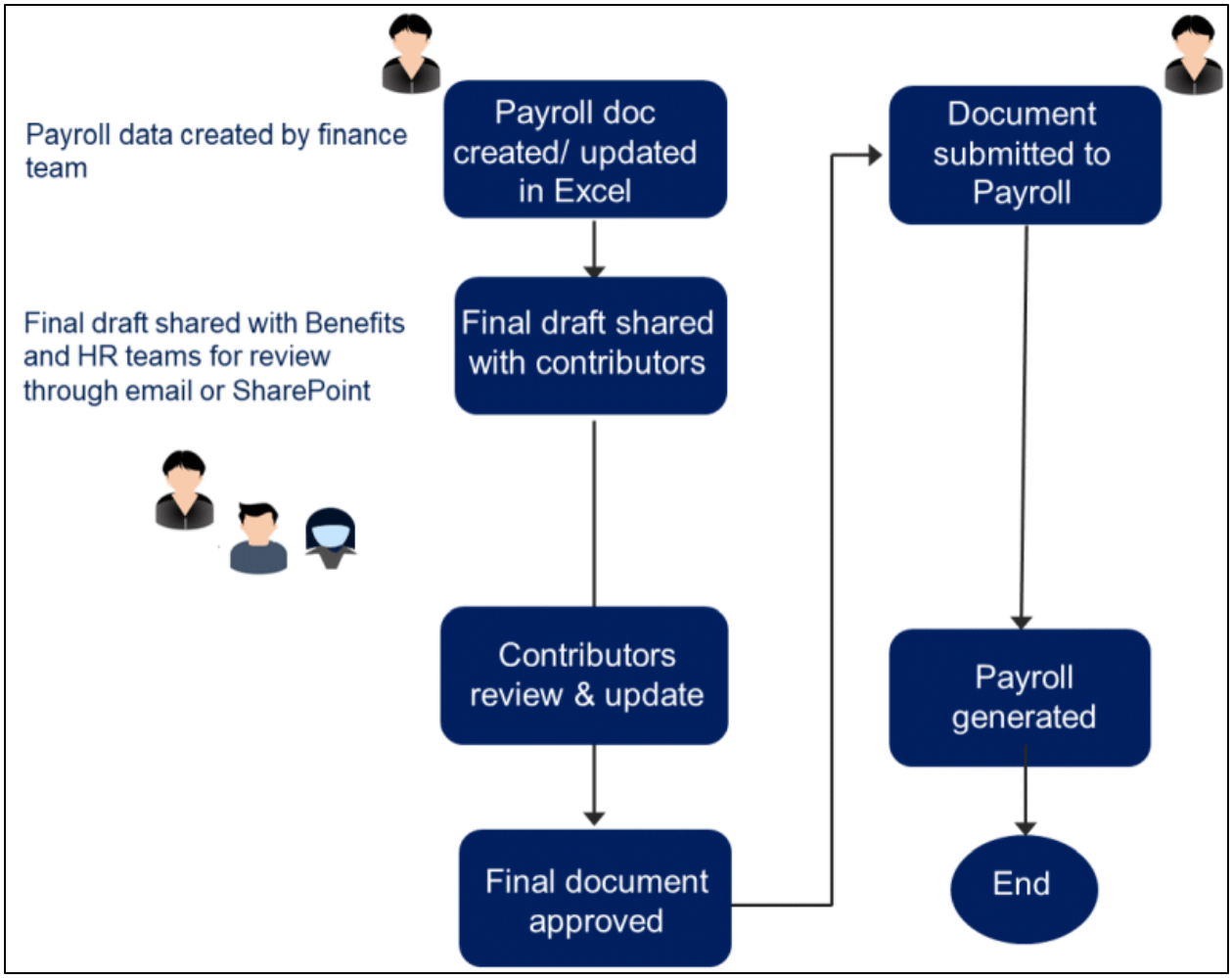
You should create use cases, scenarios, and end-user personas for all the different types of data in your organization. Interview other departments to understand what data they consider important and how they currently protect it.

When creating use cases, consider providing examples for each of these questions.

- What type of data needs protection?
  - Credit card numbers
  - Social security numbers
  - Addresses
  - Merger and acquisition negotiations
- What format?
  - Office documents (.docx, .xlsx)
  - PDF documents
  - Custom-created file format
- Where is the file located?
  - SharePoint
  - Cloud services
  - OneDrive for Business
  - Removable storage
  - Email
- How is it currently produced, maintained, and archived?
  - Generated via an automatically scheduled report
  - Data in transit via a workflow ticketing process
  - Maintained in cloud or on-premises storage
  - Past-project data archived in file or server storage

The following use case illustrates the lifecycle of a document.

1. The finance team creates a document in Excel that contains payroll data.
2. The finance team shares the final draft with the HR team via SharePoint.
3. Contributors review and update the document.
4. The finance and HR teams approve the final document and email it to the payroll team.
5. Payroll opens the document in a third-party tool for payout.



Where could you use Data Loss Prevention (DLP) in this scenario?

- Use DLP policies to block the sending of emails that contain bank account information or Social Security numbers, or optionally apply encryption automatically to the messages.
- Use Microsoft Cloud App Security to block the upload, download, or sharing of sensitive information that resides in a cloud repository
- Consider applying Rights Management service (RMS) on the SharePoint library hosting the documents.

1.2.3. Use data loss prevention (DLP) policies to protect your data

To comply with business standards and industry regulations, organizations must protect sensitive information and prevent its inadvertent disclosure. Sensitive information can

include financial data or personal information, such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically protect sensitive information across your environment.

Think of DLP as also meaning Data Lifecycle Protection. It's an opportunity to consider the entire data lifecycle, beginning with data creation. It also provides the information management/protection and security teams with a framework that describes where they want data protection and classification to be rather than concentrating on preventing loss.

There are four key areas for preventing data loss and managing the data lifecycle.

1.2.3.1. Detect/Discover.

Identify the data you want to protect. To detect sensitive data, you can use a content scan, such as Azure Information Protection (AIP) unified labeling scanner, and define data through data classification.

1.2.3.2. Protection.

Consider the range of DLP enforcement actions you can apply to documents and emails containing sensitive information, such as block sending, block sharing, warning end-users or auditing activity.

1.2.3.3. Visibility.

Protect sensitive data while keeping its visibility for appropriate uses such as:

- Forensics
- Risk management reporting
- Compliance

1.2.3.4. Data immunization.

When you apply security controls based on classification at the source (moment of creation), you can:

- Minimize data exposure time
- Provide context to help ensure that the data classification is correct

Most of your organization's data might not be RMS-protected but still require some level of DLP short of RMS encryption. AIP classification at document creation can be the start of the data protection process. An end user who applies AIP classification at document creation can assist identifying and protecting sensitive data that isn't easily detected through content inspection or other means.

1.2.4. Summary and knowledge

With Data Loss Prevention (DLP) policies in place, organizations can readily identify, monitor, and automatically protect sensitive information. You can work with key IT and business stakeholders to develop a DLP framework that helps all departments meet business requirements without burdening end users.

1.2.4.1. Check your knowledge

1.2.4.1.1.1. Question

1. Data immunization helps apply security controls to documents based on their classification at the moment of creation. Which of the following is a primary benefit of data immunization?

- Automated reporting and analytics
- Minimize the exposure time of the data
- Automated data scan and crawl
- Data cannot be stored on the dark web

1.2.4.1.1.1.1. Correct Answer

- Minimize the exposure time of the data

Correct. By using data immunization, you limit the amount of exposure time that the data is unclassified or unprotected.

1.2.4.1.1.1.2. Wrong Answer

- Automated reporting and analytics

Although you can get automated reporting and analytics when data is classified, it is not a primary benefit of immunization.

- Automated data scan and crawl

You can use Azure Information Protection Scanner to identify unlabeled or inappropriately labeled documents, but it is not a direct benefit of data immunization.

- Data cannot be stored on the dark web

Data immunization helps control data leakage by immediate classification, but it cannot prevent compromised data from being stored on the dark web

1.2.4.1.1.2. Question

2. One of the first steps to prevent data loss involves identifying data that needs protection. What Microsoft tool helps administrators detect and classify documents automatically?

- Data Loss Prevention
- Microsoft Cloud App Security (MCAS)
- SharePoint File Scanner
- Azure Information Protection Scanner

1.2.4.1.1.2.1. Correct Answer

- Azure Information Protection Scanner

Correct. You can use Azure Information Protection Scanner to identify documents in file storage that are missing or inappropriately labeled.

1.2.4.1.1.2.2. Wrong Answer

- Data Loss Prevention

Data Loss Prevention helps keep data protected and secured but will not scan through file storage to detect and classify documents.

- Microsoft Cloud App Security (MCAS)

MCAS is a cloud broker solution to help extend your security to third-party apps and services

- SharePoint File Scanner

SharePoint File Scanner is not a solution available within SharePoint or Microsoft 365.

1.2.4.1.1.3. Question

3. A security administrator needs to ensure any Excel files shared through a financial line-of-business cloud app are controlled and not shared externally. What information protection action should the security administrator take?

- Create an Azure Information Protection rule to classify all documents as confidential.
- Use Azure Information Protection Scanner
- Configure a Cloud App Security (CAS) DLP rule
- Create an Exchange transport rule

1.2.4.1.1.3.1. Correct Answer

- Configure a Cloud App Security (CAS) DLP rule

Correct. The security administrator could create a CAS DLP rule that detects and reclassifies Excel files that have been shared to OneDrive or SharePoint Online.

1.2.4.1.1.3.2. Wrong Answer

- Create an Azure Information Protection rule to classify all documents as confidential.

This would over-classify all documents and require end users to de-classify documents that they do not consider confidential.

- Use Azure Information Protection Scanner

Azure Information Protection Scanner crawls through storage to identify documents containing possible sensitive information and classify them accordingly.

- Create an Exchange transport rule

An Exchange transport rule with DLP would search for sensitive information contained in email and classify the message accordingly.

1.3.Classify data for protection and governance

1.3.1. Data classification overview

As a Microsoft 365 administrator or compliance administrator, you have several capabilities available to help you evaluate and tag content within your organization.

Understanding what sensitive content exists today in your data landscape can aid in defining labels and policies to protect and govern your data. There are various ways to do the discovery, evaluation, and tagging of content. Once labels are applied, it is important to evaluate how they are being used and what activity is occurring with this data.

1.3.1.1. Data classification solution

The data classification solution helps you classify data and report on the results. It helps you identify exposure and risks to inform policies that help you protect and govern your data. It also includes tools to manage two methods of classifying content – sensitive information types and trainable classifiers (currently in preview). Access to the solution is tightly controlled, and special permissions are required for editing and viewing. Each data classification component and its primary function is listed below:

1.3.1.1.1. Overview

Provides snapshots of how sensitive information types and labels are being used.

1.3.1.1.2. Content explorer

Explore the email and documents in your organization that contain sensitive information or have labels applied.

1.3.1.1.3. Activity explorer

Review activity related to content containing sensitive info or has labels applied, such as what labels were changed, files were modified, and more.

1.3.1.1.4. Sensitive info types

Manage the built-in and custom sensitive information types available to classify data.

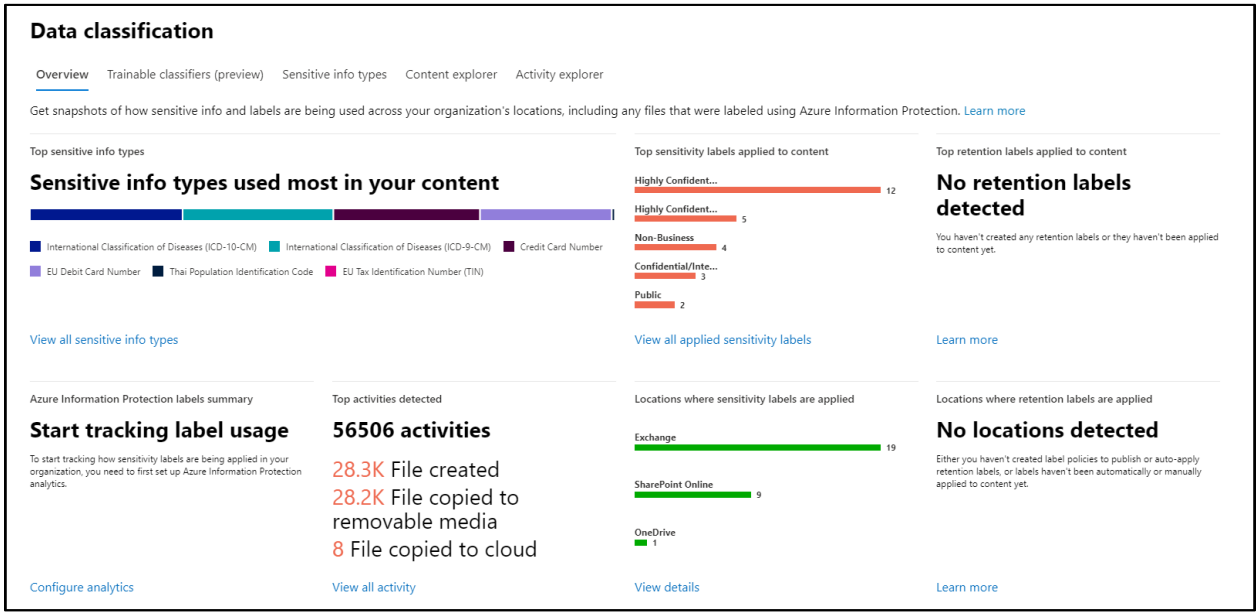
1.3.1.1.5. Trainable classifiers

Manage the classifiers used to identify content based on what the item is, not by the elements in the item.

1.3.1.2. Getting started with data classification

No configuration is needed to start identifying and classifying content containing any of the approximately 100 sensitive information type definitions included in Microsoft 365.

It happens in the background without administrator intervention. The **Top sensitive info types** card will automatically display a summary of the sensitive information discovered in SharePoint Online, OneDrive, and Exchange. Visit **Microsoft 365 compliance center > Data Classification > Overview** and look for the **Top sensitive info types** card. The image below shows the **Data classification > Overview** page prior to any configuration, with **Top sensitive info types** displaying information about what it has already discovered. The other cards are blank because no retention labels or sensitivity labels have been configured yet.



1.3.2. Classify data using sensitive information types

Using sensitive information types will most likely be a key component of your information protection and governance strategy. A sensitive information type is defined by a pattern that can be identified by a regular expression or function. They can help identify, classify, and protect content that contains credit card numbers, bank account numbers, passport numbers, and more.

1.3.2.1. Built-in and custom

Sensitive information types can be built in, customized from built-in, or created from scratch. Approximately 100 sensitive information types are built into Microsoft 365 and ready for you to use. Some built-in sensitive information types, like credit card number, are applicable to a global audience while others, like Finland National ID and Australia Driver's License Number, are specific to region or regulation. Built-in sensitive information types can be customized or created based on your organization's needs.

1.3.2.2. Key components

Sensitive information types are based on patterns, supporting evidence, character proximity, and confidence levels. A sensitive information type is defined by a pattern that can be identified by a regular expression or a function. Supporting evidence such as keywords and checksums can also be used to identify a sensitive information type. Confidence level and character proximity are also used in the detection process.

The built-in sensitive information types are described using these characteristics:

1.3.2.2.1. Format

General description of sensitive information type. Here are three examples:

- 14 to 16 digits that can be formatted or unformatted and which must pass the Luhn test
- Nine digits with optional forward slash (old format) 10 digits with optional forward slash (new format)
- One letter (in English) followed by nine digits

1.3.2.2.2. Pattern

Adds more detail to **Format**. An example of a pattern is one letter (in English) followed by nine digits:

- One letter (in English, not case sensitive)
- The digit "1" or "2"
- Eight digits

1.3.2.2.3. Checksum

Some sensitive information types use checksums for error detection, while others don't.

1.3.2.2.4. Keywords

Text-based words or phrases that typically act as supporting evidence to confirm a pattern match. Here are some examples:

- ID Number
- License number
- Patient number

1.3.2.2.5. Definition

The confidence level, stated in percentage terms, in which Microsoft 365 has detected a sensitive information type based on a set of conditions being met within a specific character proximity. A sensitive information type can have more than one definition, each with a different confidence level. Conditions are based on:

- Content matches the pattern
- A keyword is found
- The checksum (if it exists) passes

1.3.2.3. Policy integration

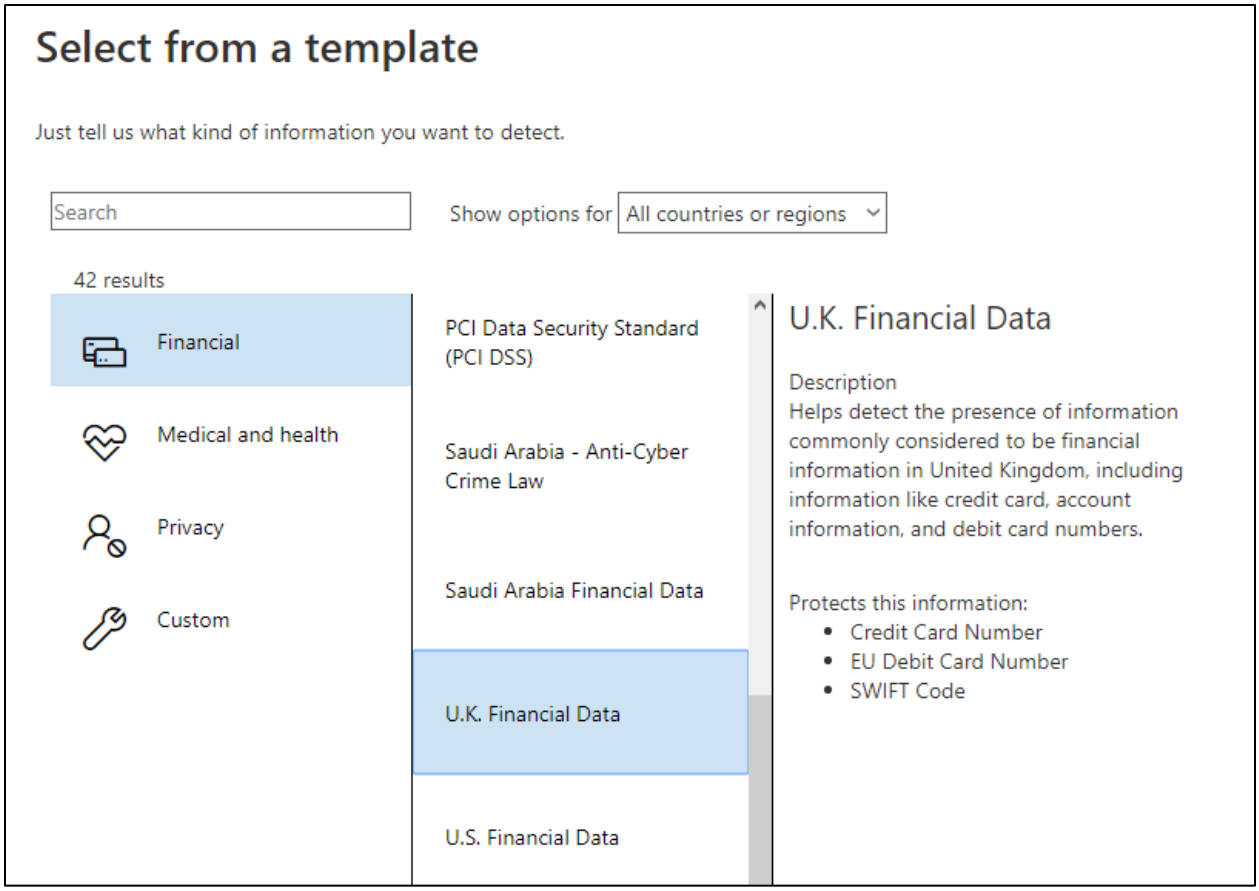
Sensitive information types can be used on their own to classify data. They can also be specified in conditions (individually or grouped into a policy template) to configure policies in Microsoft's solutions for information protection and governance. The table below shows each of the information protection and governance solutions and where in those solutions you can use sensitive information types.

Solution	Where used
Information protection	Sensitivity label auto-labeling policies
Data loss prevention (DLP)	DLP policies
Information governance	Retention policies and Retention label auto-apply policies
Records management	Retention label auto-apply policies

A policy template contains a group of related sensitive information types. You can use policy templates to simplify policy creation. Policy template selection is an optional part of all the policy processes listed above. Microsoft 365 includes 42 policy templates divided into three categories: financial, medical and health, and privacy. You can also filter the templates by a specific country or region.

The image below shows the policy template selection screen from the retention label auto-apply policy wizard. You can see the U.K. Financial Data policy template detects these sensitive information types:

- Credit Card Number
- EU Debit Card Number
- SWIFT Code



1.3.3. Classify data using trainable classifiers

Most organizations have content to protect that cannot be detected using the methods used by sensitive information types. Data classification using trainable classifiers (currently in preview) is useful when content is not easily identified using pattern matching. Trainable classifiers apply the power of artificial intelligence (AI) and machine learning (ML) to find data to track, protect, and govern. You train a classifier to identify sensitive content based on what it is, rather than the elements in the item.

1.3.3.1. Licensing for trainable classifiers

This feature is a capability included with:

1. Microsoft 365 E5
2. Microsoft 365 E5 Compliance
3. Microsoft 365 E5 Information Protection and Governance

Please review Microsoft 365 licensing guidance for security & compliance to identify required licenses for your organization.

1.3.3.2. Built-in classifiers

Microsoft 365 comes with five classifiers already trained and ready to use.

- Résumés
- Source Code
- Harassment
- Profanity
- Threat

You should test the built-in classifiers to determine if they are working as you expect prior to applying them to a large audience or significant amount of content.

1.3.3.3. Custom trainable classifiers

You can create and train your own classifiers to look for data unique to your organization such as customer records, human resources data, and contracts. Creating a trainable classifier can take a significant amount of time and requires careful preparation.

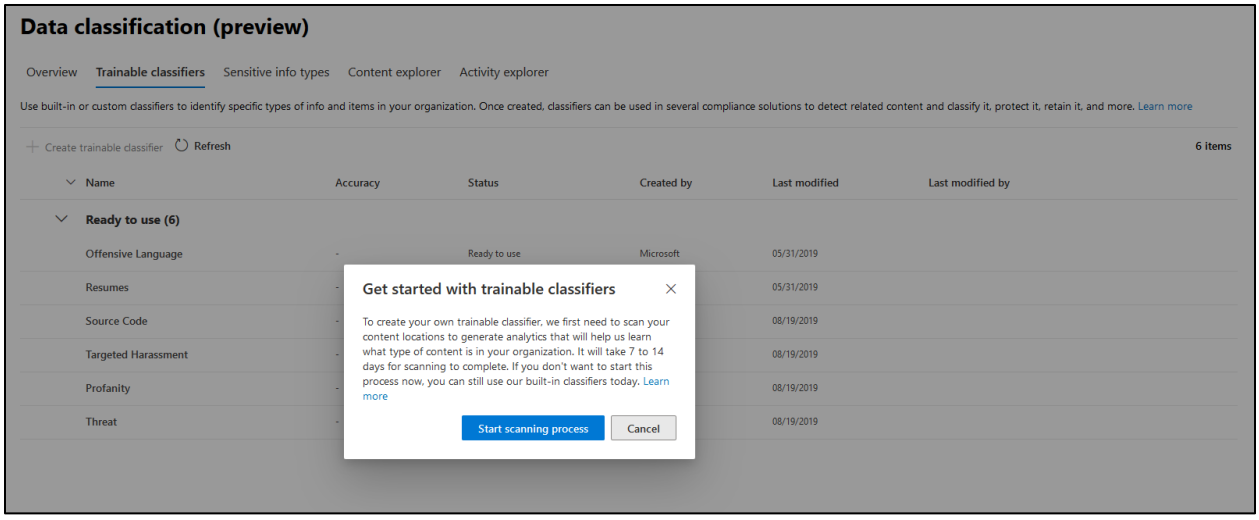
Once the one-time setup process is complete, you can begin configuring trainable classifiers. The trainable classifier configuration process can be broken down as follows:

1. **Seed**. Prepare your sample data and create the trainable classifier.
2. **Test**. Prepare test data, test the predictive model, and evaluate the results.
3. **Publish**. Make the trainable classifier available for use in your compliance solutions.

Each step is explained in more detail below.

1.3.3.3.1. One-time setup

A one-time scan must be completed before creating any custom trainable classifiers. This is needed so Microsoft 365 can learn more about the content in your organization. *This process takes 7 to 14 days*. The image below shows the message you will receive when attempting to create a custom trainable classifier for the first time.



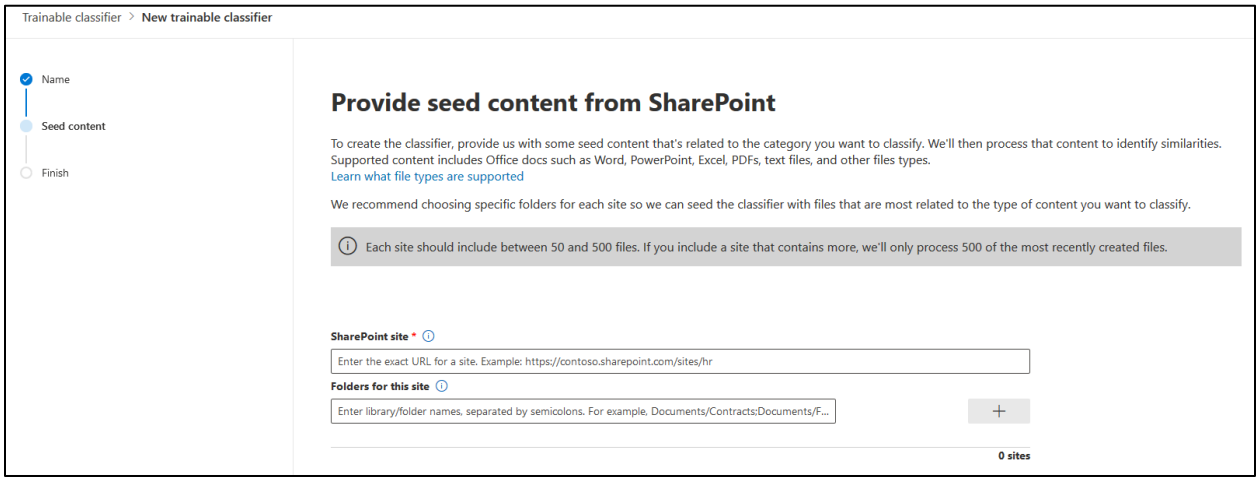
1.3.3.3.1.1. Seed

1.3.3.3.1.1.1. Step 1: Prepare sample data.

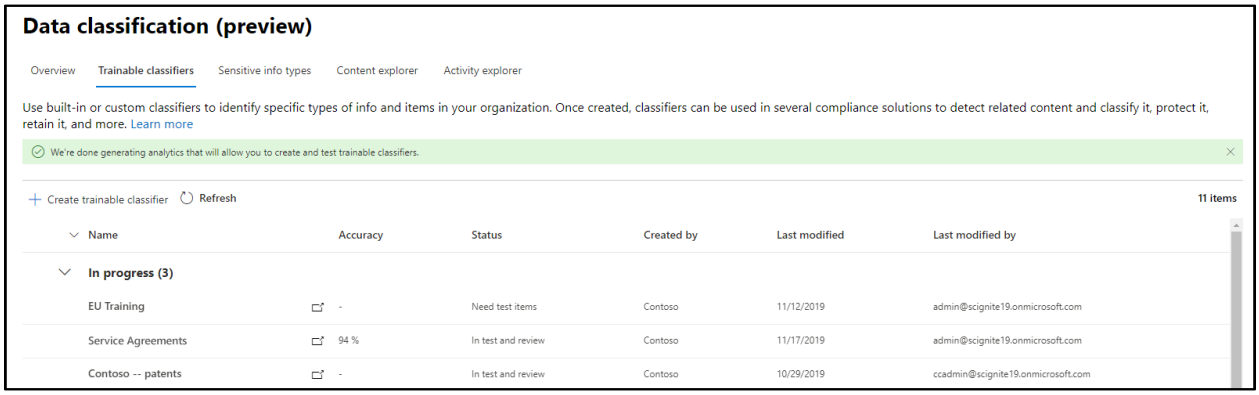
Prepare content to seed your predictive model consisting of known positive samples of the content you want to classify and store it in a SharePoint Online document library or folder. You will need at least 50 and as many as 500 samples that strongly represent the type of content you want the trainable classifier to detect.

1.3.3.3.1.1.2. Step 2: Create trainable classifier.

Create the classifier by navigating to Microsoft 365 compliance center > Data classification > Trainable classifiers > Create trainable classifier. You will give the classifier a name, a description, and provide the location of the seed content. The image below shows the Provide seed content from SharePoint page in the Create new classifier wizard.



It can take as long as 24 hours for the prediction model to be built once you complete the **Finish** step in the **Create trainable classifier** wizard. The image below shows the **EU Training** trainable classifier with a status of **Need test items**. That means the seed content has been processed and the predictive model is ready for testing.



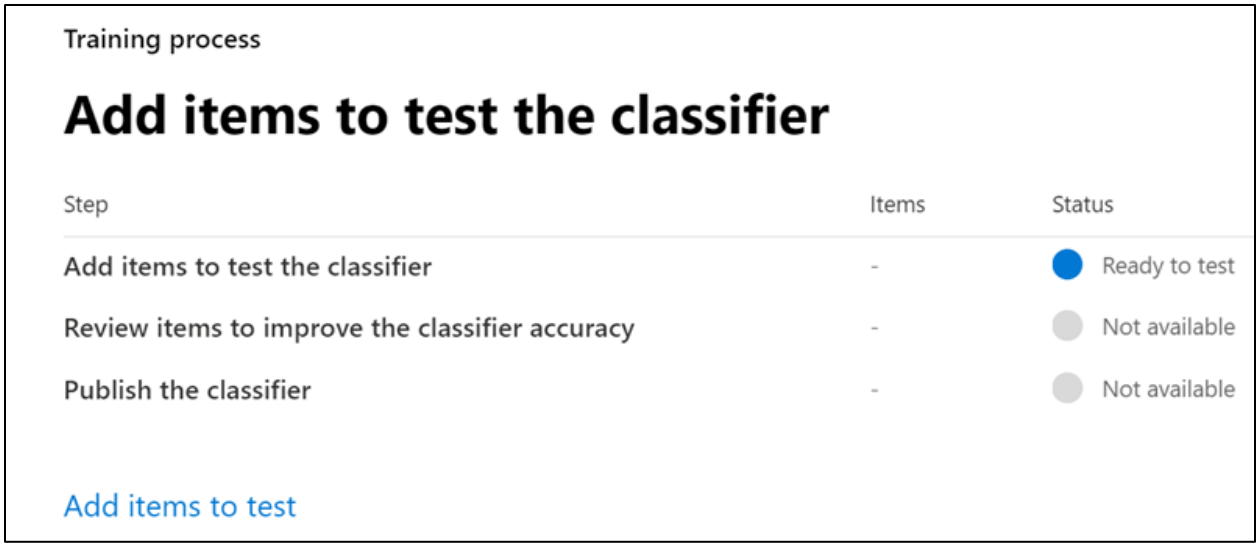
1.3.3.3.1.2. Test

1.3.3.3.1.2.1. Step 1: Prepare test data.

Start testing the predictive model once seeding is complete. You need at least 200 and as many as 10,000 positive and negative examples of the content you are training the classifier to detect. The content used to build the model should not be used to test the model. Create a second SharePoint document library or folder for the test content, move your content there, and wait for the folder to be indexed.

1.3.3.3.1.2.2. Step 2: Test predictive model.

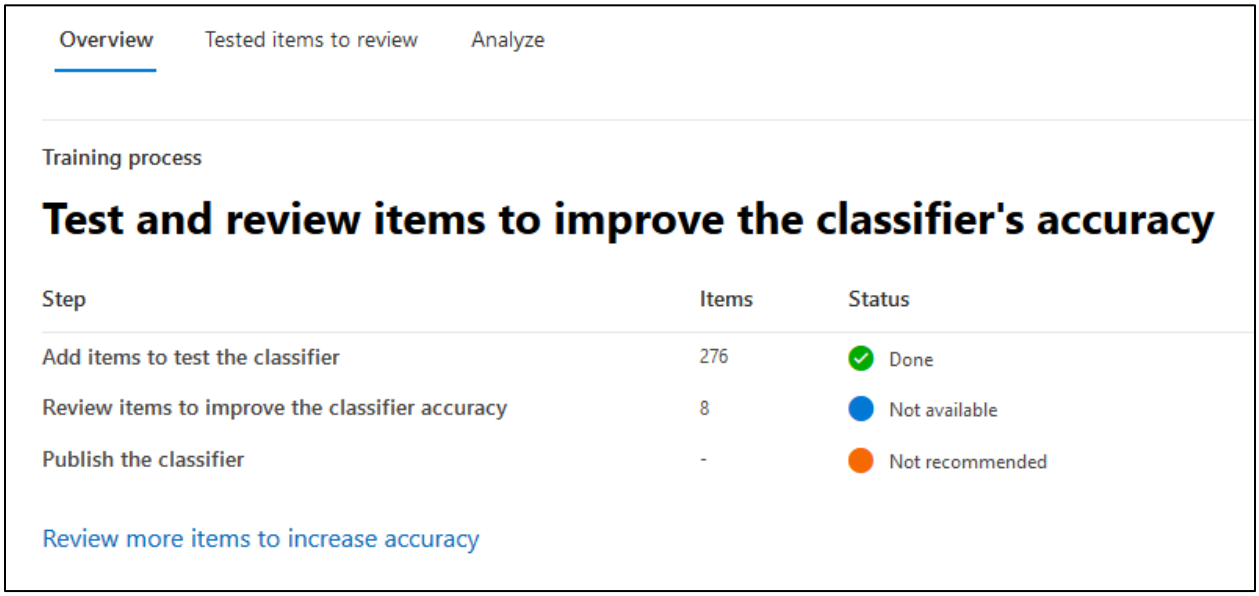
You start the test wizard by clicking on Add items to test on the trainable classifier information page. Point to the SharePoint site holding the test items and choose Done to start the test. The image below shows the Training process card on the trainable classifier information page before you start the testing process. Notice the status is Ready to test. Once you begin the test, Microsoft 365 attempts to predict whether each item you provided for testing is Relevant or Not Relevant.



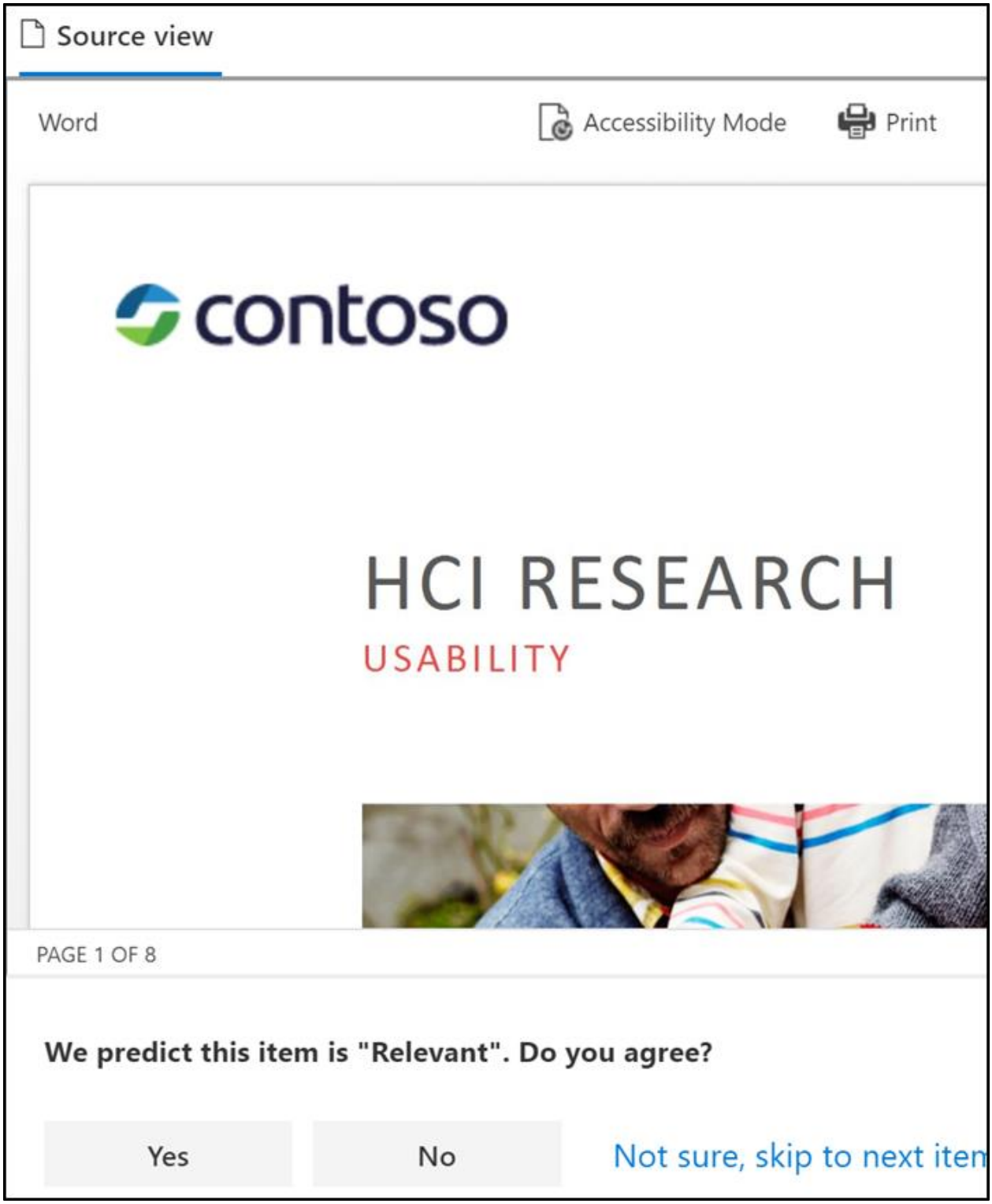
1.3.3.3.1.2.3. Step 3: Evaluate predictions.

You need to tell the model if it is accurately predicting the relevance of the test content when the trainable classifier is done processing your test data. The Review items to improve the classifier accuracy step will be set to Ready to review when it is ready for you to conduct the evaluation.

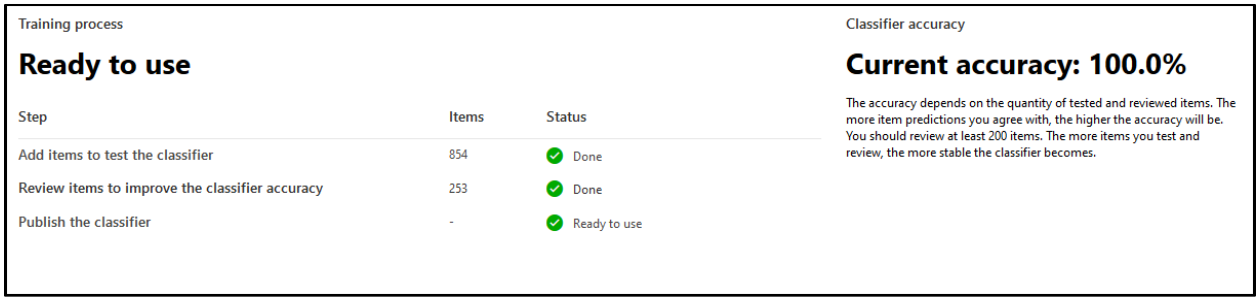
The image below shows the review process is currently underway with 8 test items reviewed so far. The status is Not available because not enough test content has been evaluated yet.



Choose the **Tested items to review** tab to review and evaluate items. You will be presented with 30 items to review at a time. You review each item and determine if the predictive model correctly classified the item. The image below shows one of the test documents undergoing an evaluation to determine if it is relevant. You choose **Yes**, **No**, or **Not sure**, **skip to the next item**. Model accuracy improves with every item you evaluate. You should review at least 200 items.



Once you have reviewed enough items and accuracy reaches at least 70%, you can publish the trainable classifier or continue to improve the accuracy of the model by conducting additional testing and evaluation.



1.3.3.3.1.3. Publish

Publish the trainable classifier when you are satisfied with the results from the predictive model. Once published, your custom trainable classifier will be available in selected compliance solutions. The status for a published trainable classifier is **Ready to use**.

1.3.4. Review sensitive information and label usage

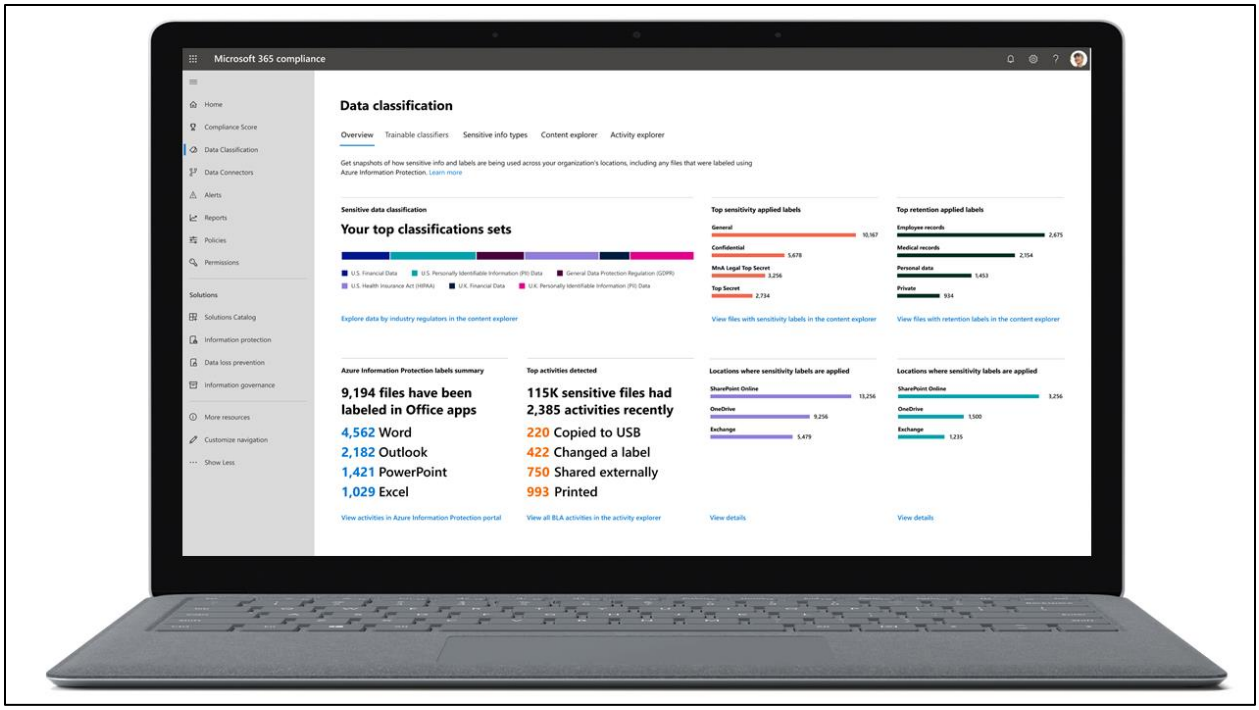
The data classification **Overview** page provides snapshots of how sensitive information and labels are being used in your organization. It displays the volume of sensitive data across Exchange, SharePoint, and OneDrive. The view is categorized by sensitive information types, like US Social Security Number, Credit Card Number, and IP Address.

The **Overview** page can answer questions like:

- What sensitive data is out there?
- What labels are being used the most?
- Is sensitive data being copied or shared outside the organization?

You can complete the following tasks in the overview section:

- Examine the volume and location of sensitive and business critical information.
- Monitor risky activities associated with sensitive information to inform DLP policies.
- Understand label utilization across Microsoft 365 to improve protection and governance policies.



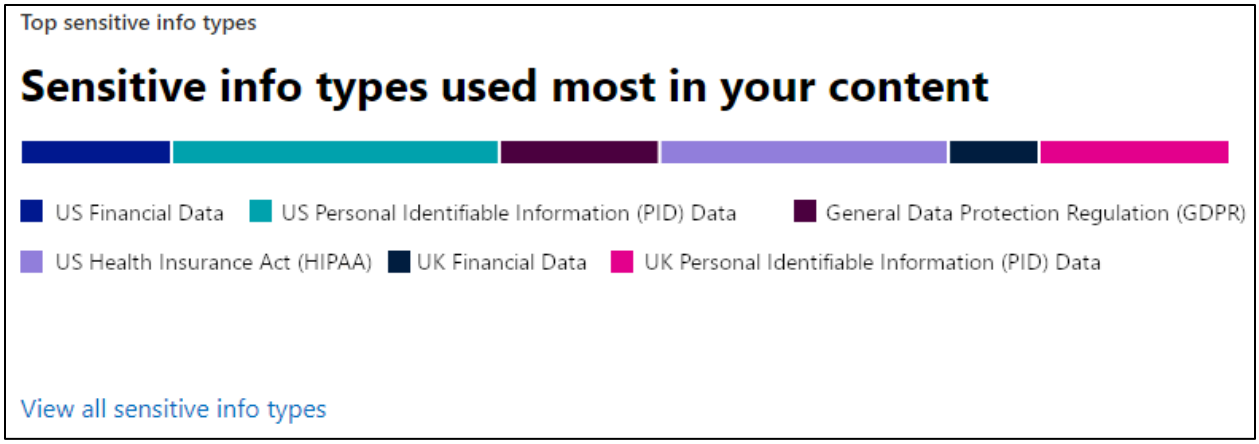
The Overview page includes the following cards:

1. Top sensitive info types
2. Top sensitivity labels applied to content
3. Top retention labels applied to content
4. Top activities detected
5. Locations where sensitivity labels are applied
6. Locations where retention labels are applied
7. Azure Information Protection labels summary

Each card, except for the Azure Information Protection labels summary, links to either the Activity explorer or Content explorer, where a more thorough examination of the data can be done.

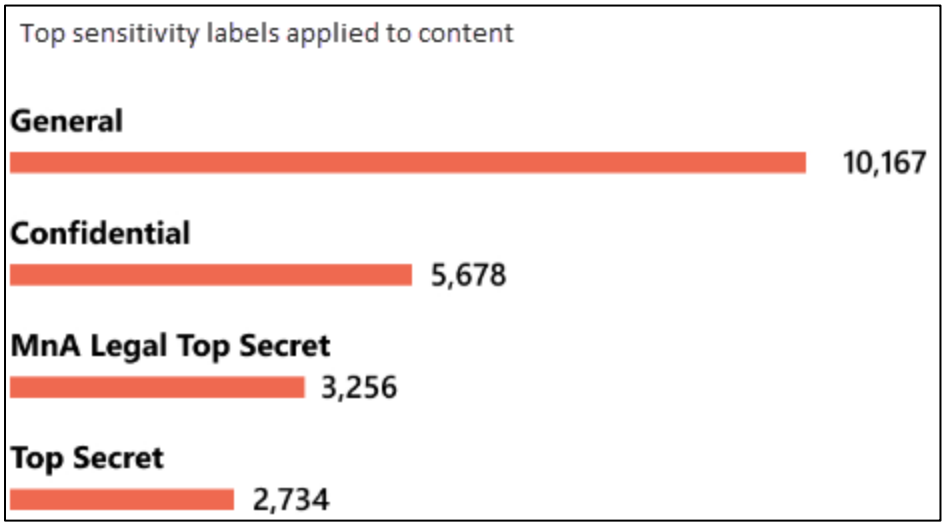
1.3.4.1. Top sensitive info types

The **Top sensitive info types** card shows the top sensitive information types discovered in the organization. This card will be visible if Microsoft 365 has identified any sensitive information types in SharePoint Online, Exchange Online, and OneDrive. No setup or configuration is required. You can use the information on the sensitive information types discovered to help you determine what labels and policies to create. The **View all sensitive info** types link takes you to the **Content explorer**.



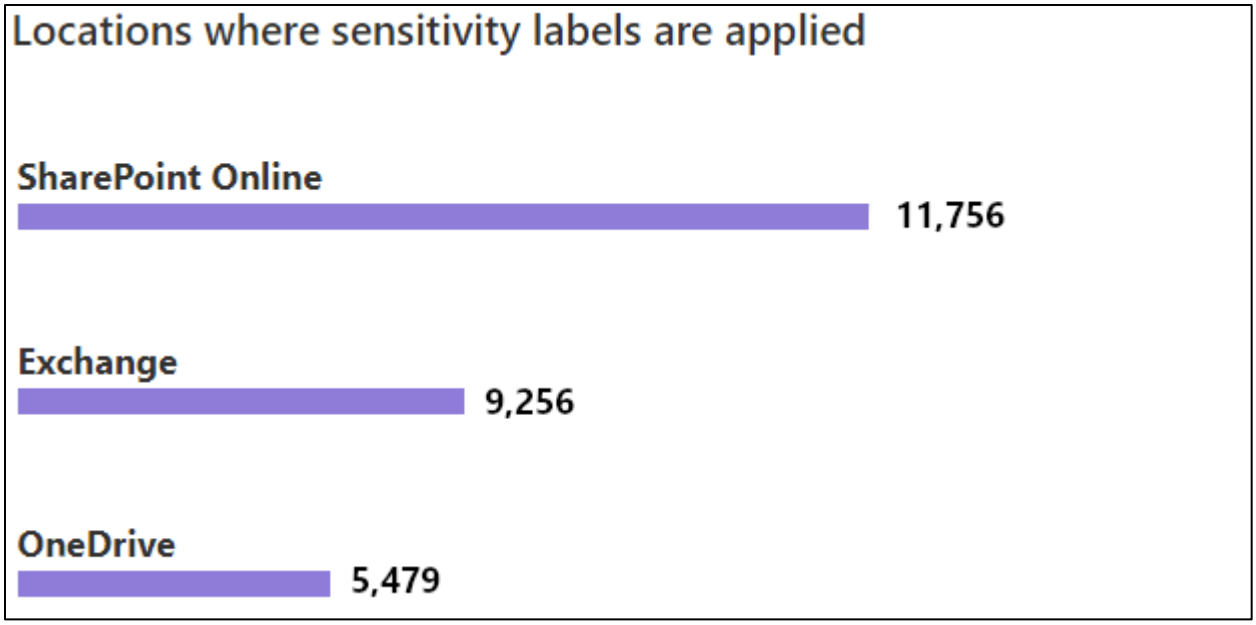
1.3.4.2. Top sensitivity labels applied to content

The **Top sensitivity labels applied to content** card show the sensitivity labels most frequently applied to content, grouped by sensitivity label. This card will display **No sensitivity labels detected** if you have not created any sensitivity labels or they have not been applied to any content.



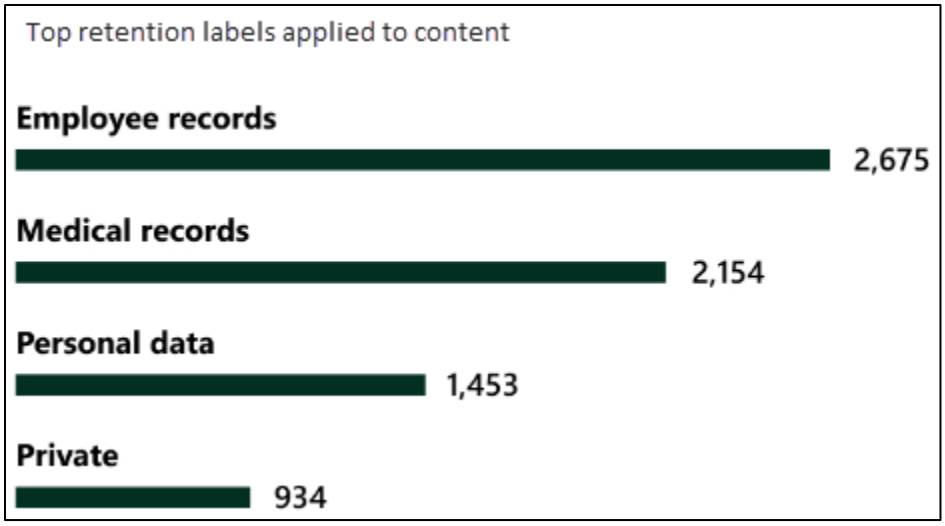
1.3.4.3. Locations where sensitivity labels are applied

This card shows the number of items with a sensitivity label applied grouped by location like SharePoint Online, Exchange Online, and OneDrive. At least one item must have a sensitivity label applied for this card to show any information.



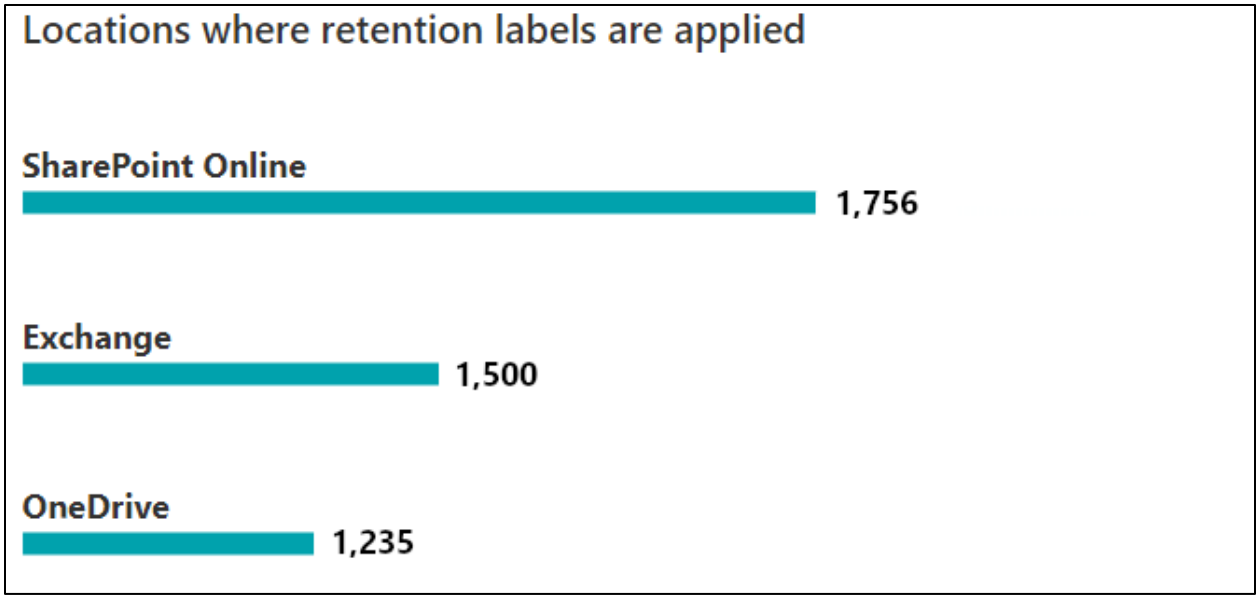
1.3.4.4. Top retention labels applied

The **Top retention labels applied** to content card shows the most frequently applied retention labels, grouped by retention label. At least one item must have a retention label applied for this card to be populated.



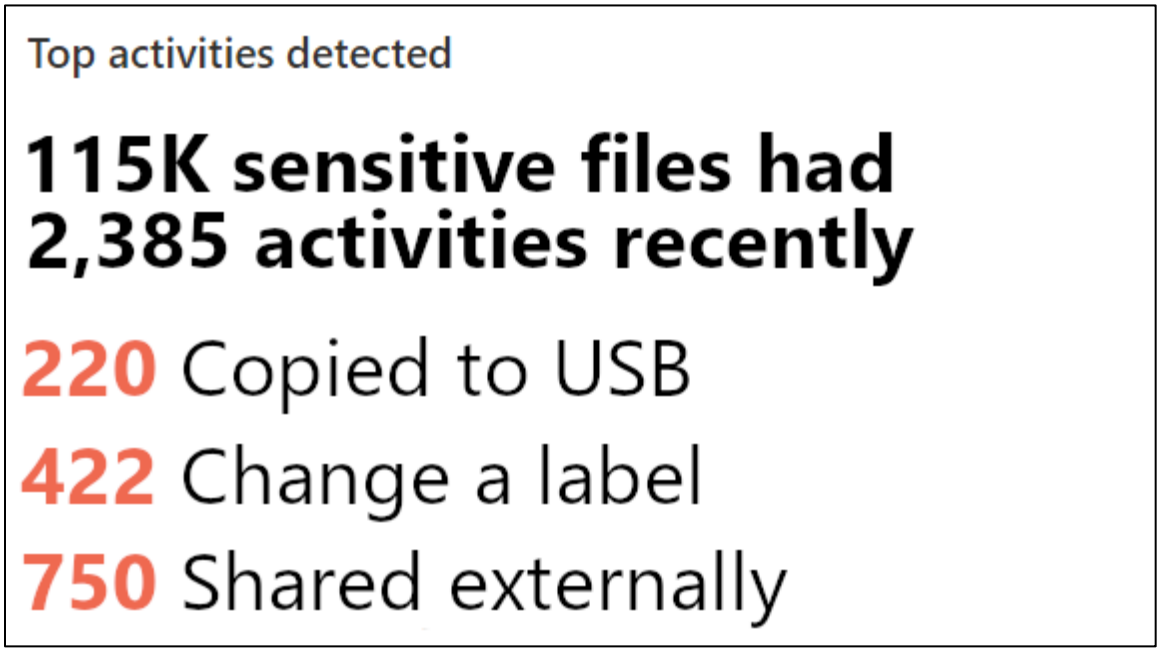
1.3.4.5. Locations where retention labels are applied

The **Locations where retention labels are applied** card shows the number of items with a retention label applied, grouped by location. At least one item must have a retention label applied for this card to be populated.



1.3.4.6. Top activities detected

The **top activities detected** card summarizes the most common actions taken on items with sensitivity labels applied. This card helps you understand what users are doing with the organization's sensitive data.

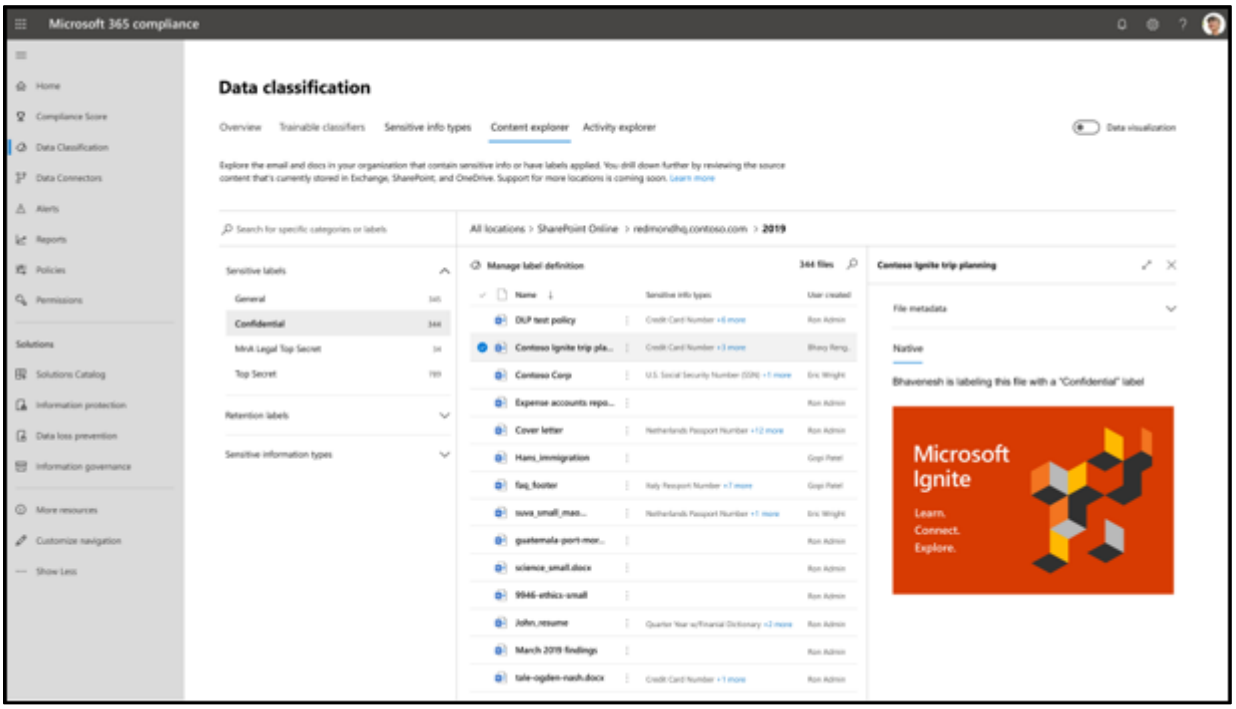


1.3.5. Explore labeled and sensitive content

1.3.5.1. Content explorer

shows a current snapshot of items with a sensitivity label or retention label applied, or that have been classified as containing a sensitive information type. Here is a summary of what the content explorer provides:

- Visibility into the amount of sensitive data in a document that triggered the classification to be applied.
- Ability to filter by label or sensitive information type to get a detailed view of the locations where the data is stored.
- Integrated viewer to display documents, providing context for the circumstances in which sensitive information is being detected.

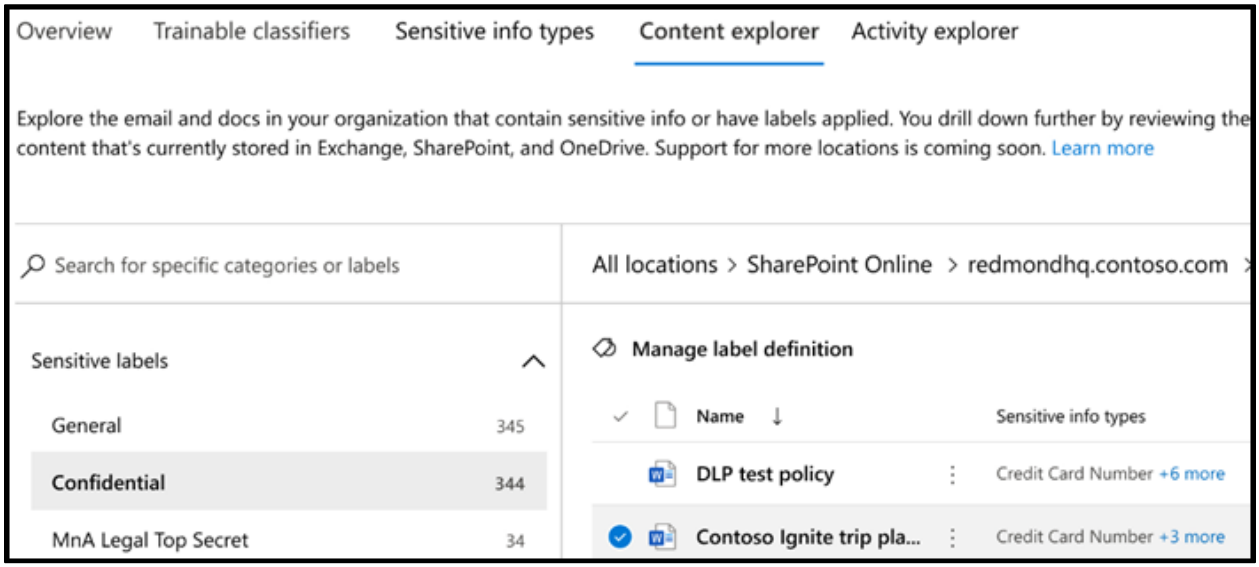


This feature is a capability included with:

- Microsoft 365 E5
- Microsoft 365 E5 Compliance
- Microsoft 365 E5 Information Protection and Governance

Please review Microsoft 365 licensing guidance for security & compliance to identify required licenses for your organization.

You can search for specific sensitive information types, sensitivity labels or retention labels, or browse to the one you are interested in. The right side of the page will summarize the number of items meeting the classification you selected grouped by location. Additional information is available by listing the specific items matching the label or sensitive information type and viewing the source content stored in Exchange, SharePoint, and OneDrive. Each of these activities (listing and viewing) requires additional permissions due to the potentially sensitive nature of the content.



1.3.6. Understand activities related to your data

1.3.6.1. Activity explorer

Activity explorer gives you a better understanding of activities related to your data. It provides visibility into document-level activities like label changes and label downgrades (like when someone changes a label from confidential to public). You can use the filters to see all the details for a specific label, including file types, users, and activities. Activity explorer enables you to understand what is being done with your labeled content over time. You can use activity explorer to evaluate if the controls already in place, such as DLP policies, are effective. You can update your policies and take action to restrict undesired behavior if you discover something unexpected.

This feature is a capability included with:

- Microsoft 365 E5
- Microsoft 365 E5 Compliance
- Microsoft 365 E5 Information Protection and Governance

Please review Microsoft 365 licensing guidance for security & compliance to identify required licenses for your organization.

Here are the activity types available for analysis.

- File created
- File modified
- File renamed
- File copied to cloud
- File accessed by unallowed app
- File printed
- File copied to removable media
- File copied to network share
- File read
- File copied to clipboard
- Label applied
- Label changed

You can filter data by:

- date range
- activity type
- location
- user
- sensitivity label
- retention label

Understanding the activities users are performing on sensitive information helps you identify the right information protection and DLP policies to apply to secure your content.

Activity explorer provides the following:

- Visibility into document-level activities like label changes and label downgrades.
- Ability to filter to see all the details for a specific label including file types, users, and activities.
- Understand a broad-spectrum of sensitivity label activities across Microsoft 365.

1.3.7. Summary and knowledge

Your data starts with discovering and classifying the emails and documents in your digital estate. The information and tools available in the Data Classification Solution in the Microsoft 365 compliance center help you understand the sensitive information you have and how it is being used.

Now that you have completed this module, you should be able to:

- List the components of the Data Classification solution.
- Identify the cards available on the Data Classification overview tab.
- Explain the Content explorer and Activity explorer.
- Describe how to use sensitive information types and trainable classifiers.

1.3.7.1.1.1. Question

1. Where do you go in the data classification dashboard to explore the email and docs in your organization that contain sensitive information or have labels applied?

- Activity explorer
- Content explorer
- Sensitive info types

1.3.7.1.1.1.1. Correct Answer

- Content explorer

Content explorer shows a current snapshot of the items that have a sensitivity label, a retention label, or have been classified as a sensitive information type.

1.3.7.1.1.1.2. Wrong Answer

- Activity explorer

The activity explorer shows document-level activities like label changes and label downgrades, such as from confidential to general, across various locations. Intelligent detections.

- Sensitive info types

Sensitive info types are where you manage the built-in and custom sensitive information types available to classify data.

1.3.7.1.1.2. Question

2. You can create custom sensitive information types for data specific to your organization. Which of the following statements is true regarding creating new custom sensitive information types?

- You cannot assign higher levels of confidence for your custom sensitive information type.
- You can use Exact Data Match (EDM)-based classification.
- You can only use the features that are customized.

1.3.7.1.1.2.1. Correct Answer

- You can use Exact Data Match (EDM)-based classification.

You can set up custom sensitive information types using Exact Data Match (EDM)-based classification.

1.3.7.1.1.2.2. Wrong Answer

- You cannot assign higher levels of confidence for your custom sensitive information type.

The more supporting evidence you have, the higher the likelihood that a match contains the sensitive information you're looking for. You can assign higher levels of confidence for matches that are detected by using more evidence.

- You can only use the features that are customized.

Sensitive information types can be built in, customized, or created from scratch.

1.3.7.1.1.3. Question

3. Which of the following can be completed from the data classification overview page?

- Filter by label or sensitive type to get a detailed view of locations where data is stored.
- Filter to see all the details for a specific label including file types, users, and activities.

- Monitor risky activities associated with sensitive information to inform DLP policies.

1.3.7.1.1.3.1. Correct Answer

- Monitor risky activities associated with sensitive information to inform DLP policies.

The data classification overview page provides snapshots of how sensitive info and labels are being used across your organization's locations. The overview page shows volume of sensitive data across Exchange Online, SharePoint Online, and OneDrive for Business, categorized by sensitive information types such as social security number (SSN), or associated with regulations like the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Health Insurance Portability and Accountability Act (HIPAA).

1.3.7.1.1.3.2. Wrong Answer

- Filter by label or sensitive type to get a detailed view of locations where data is stored.

You can search for specific sensitive information types, sensitivity labels or retention labels, or browse to the one you are interested in via the content explorer.

- Filter to see all the details for a specific label including file types, users, and activities.

Activity explorer enables you to understand what is being done with your labeled content over time. You can use activity explorer to evaluate if the controls already in place, such as data loss prevention policies, are effective.

1.3.7.1.1.4. Question

4. Which card on the data classification overview tab shows the number of items with a retention label applied grouped by location?

- Locations where retention labels are applied.
- Top activities detected
- Top sensitive information types

1.3.7.1.1.4.1. Correct Answer

- Locations where retention labels are applied.

The locations where retention labels are applied card shows the number of items with a retention label applied grouped by location.

1.3.7.1.1.4.2. Wrong Answer

- Top activities detected

The top activities detected card summarizes the most common actions on items with sensitivity labels applied.

- Top sensitive information types

The top sensitive info types card shows the top sensitive information types discovered and labeled in the organization.

1.3.7.1.1.5. Question

5. Trainable classifiers use which of the following to identify what an item actually is?

- Metadata
- Machine learning
- Keywords

1.3.7.1.1.5.1. Correct Answer

- Machine learning

Trainable classifiers use machine learning to identify what an item actually is. It does this by analyzing hundreds of examples of a type of content (such as an invoice), which you provide to the engine.

1.3.7.1.1.5.2. Wrong Answer

- Metadata

Unlike pattern matching, trainable classifiers do not look at metadata.

- Keywords

Unlike pattern matching, trainable classifiers do not look at keywords.

1.4.Create and manage sensitive information types

1.4.1. Introduction

Finding sensitive data between all the data produced in an organization requires different search and recognition patterns, which are called sensitive information types. In this module, you will learn how to use sensitive information types to support your information protection strategy.

A sensitive information type is defined by a pattern that can be identified by a regular expression or a function. In addition, corroborative evidence such as keywords and checksums can be used to identify a sensitive information type. Confidence level and proximity are also used in the evaluation process. Altogether, these elements serve as the foundation of the various policies you will establish in Microsoft 365 to protect your information and support your information governance strategy.

1.4.1.1. Learning objectives

Upon completion of this module, you should be able to:

- Recognize the difference between built-in and custom sensitivity labels
- Configure sensitive information types with exact data match-based classification
- Implement document fingerprinting
- Create custom keyword dictionaries

1.4.1.2. Prerequisites

- Basic understanding of the Microsoft 365 services
- Basic understanding information protection and governance in Microsoft 365

1.4.2. Compare built-in versus custom sensitive information types

Sensitive information types are used to identify sensitive items. Credit card number and EU debit card number are examples of sensitive information types. Sensitive information types look for specific patterns. Sensitive information types validate the data by looking

at its format, its checksums, and look for relevant keywords or other information. Some of this functionality is performed by internal functions.

Microsoft 365 provides more than 100 built-in sensitive information types, that can help to identify and protect credit card numbers, bank account numbers, passport numbers, and more, based on patterns that are defined by a regular expression (regex) or a function. These built-in definitions can help organizations to quickly deploy solutions in Microsoft 365 to protect company data, using data loss prevention (DLP), retention labels and policies and sensitivity labels.

While the built-in sensitive information types help organizations to quickly identify commonly used types of sensitive data, some sensitive information is organization-specific and require custom sensitive information types. For example, employee IDs, project numbers or other key values of intellectual property may be important to certain industry sectors. To find and protect this information, organizations can create a custom sensitive information type.

1.4.2.1. Sensitive information type parts

The fundamental components of sensitive information types are the same for built-in and custom sensitive information types and described in the following table:

1.4.2.1.1. Component

For example, the sensitive information type search pattern for a " U.S. social security number (SSN)" is defined as the following:

- It uses four different functions to search for different regular expressions).
- When a regular expression is matched and within 300 characters of a keyword from the *Keyword_ssn* list, this adds more evidence by proximity.

Whenever possible, use the built-in sensitive information types first, because your organization will benefit from the Microsoft managed data matching patterns from the start.

1.4.2.1.1.1. Primary Pattern

Employee ID numbers, project numbers, etc. This is typically identified by a regular expression (RegEx), but it can also be a list of keywords.

1.4.2.1.1.2. Additional evidence

Suppose you're looking for a nine-digit employee ID number. Not all nine-digit numbers are employee ID numbers, so you can look for more text with keywords like "employee", "badge", "ID", or other text patterns based on other regular expressions. This supporting evidence (also known as supporting or corroborative evidence) increases the likelihood that nine-digit number found in content is really an employee ID number and lowers the chance for false positives.

1.4.2.1.1.3. Character proximity

The closer the primary pattern and the supporting evidence are to each other, the more likely the detected content is going to be what you are looking for. You can specify the character distance between the primary pattern and the supporting evidence, that is also known as the proximity window. This is another factor to reduce false positives and increases the accuracy of finding actual sensitive information to protect.

1.4.2.1.1.4. Confidence level

The more supporting evidence you have, the higher the likelihood that a match contains the sensitive information you are looking for. You can assign higher levels of confidence for matches that are detected by using more evidence. However, this also raises the number of false positives.

1.4.2.2. Custom sensitive information type features

Typically, organizational requirements can be fulfilled using the built-in sensitive information types such as protecting customer credit card numbers or employees and customer personal information from accidental sharing. However, organizations may still need to protect custom sensitive data with custom sensitive information types. These requirements may include the need to protect exact data matches from spreadsheets or documents being shared.

The special features of custom sensitive information types include:

- Exact Data Match (EDM)-based classification
- Document Fingerprinting
- Keyword dictionaries

The following table explains the use cases for the three special features:

Feature	What is it?	When to use it?	Recommendation
Exact Data Match (EDM)-based classification	Enables the creation of databases with custom sensitive information types that refer to exact values. The database can be refreshed daily and contain up to 100 million rows of data.	When large quantities of sensitive information need to be matched daily, for example all the stored personal information of employees of an organization. EDM-based classification enables you to find exact data matches. For example, if the first- and family name and the date of birth of a certain employee is sent in a message, EDM classification can match this information from its database of sensitive information.	Best for organizations that need to store large amounts of personal information, such as hospitals, can benefit from EDM-based classification to make sure no personal information of patients are being shared.
Document Fingerprinting	Converts a standard form into a sensitive information type.	A document fingerprint can be created on a blank patent template, Government forms or Employee information forms for Human Resources departments. Whenever the same template is used for creating a new form, the custom sensitive information type is matched independently from the rest of the content.	Ideally, organizations already have an established business practice of using certain forms to transmit sensitive information. After uploading an empty form to be converted to a document fingerprint, and then set up a corresponding policy, any documents in outbound mail or being shared, that match that fingerprint, are detected.

Feature	What is it?	When to use it?	Recommendation
Keyword dictionaries	Keyword dictionaries provide a simple solution for managing reused keyword lists for matching of company information at a large scale, supporting up to 1 MB of keywords in any language.	When identifying generic content, such as healthcare-related communication (ICD classification) or inappropriate or explicit language, keyword dictionaries can be used to detect certain words and take actions on them, such as preventing loss or enforcing company guidelines.	Keyword dictionaries are not as accurate as EDM-based classification, because they only provide simple keywords detection, but they are useful when organizations need to detect industry-specific terms before they are shared with internals or externals or to enforce company guidelines.

Most organizations should start with the built-in sensitive information types for general protection against data loss of most common sensitive data. Then organizations should analyze their individual needs to protect specific data by creating custom sensitive information types. Afterwards organizations should then use the advanced features of custom sensitive information types, to increase accuracy and simplify management.

1.4.3. Create and manage custom sensitive information types

A common usage scenario for a custom sensitive information type is to protect stored employee IDs, cost center numbers, and other human resources and finance department-specific data against accidental loss. Since most organizations use individual patterns for this information, they cannot use a default built-on sensitive information type.

Instead, they need to create a custom sensitive information type to use at a later stage of implementation in a data loss prevention policy, a sensitivity label, or for a retention policy or label.

The best way to create a new custom sensitive information type is to search for an existing built-in sensitive information type that functions like your needs, export, and modify the rule and upload it with a new name.

Regular Expressions are a powerful tool. Creating search patterns is a recurring task. For more information see the resources available at the end of this module for more details on using regular expressions.

1.4.4. Describe custom sensitive information types with exact data match

EDM-based classification enables you to create custom sensitive information types that refer to exact values in a database of sensitive information. The database can be refreshed daily and contain up to 100 million rows of data. So as employees, patients, or clients come and go, and records change, your custom sensitive information types remain current and applicable.

Creating a new custom sensitive information type with EDM-based classification involves the following steps performed in order:

1. Set up EDM-based classification
2. Hash and upload the sensitive data
3. Use EDM-based classification with your Microsoft cloud services.

1.4.5. Implement document fingerprinting

Information workers in your organization handle many kinds of sensitive information during a typical day. Document Fingerprinting in Microsoft 365 makes it easier for you to protect this information by identifying standard forms that are used throughout your organization.

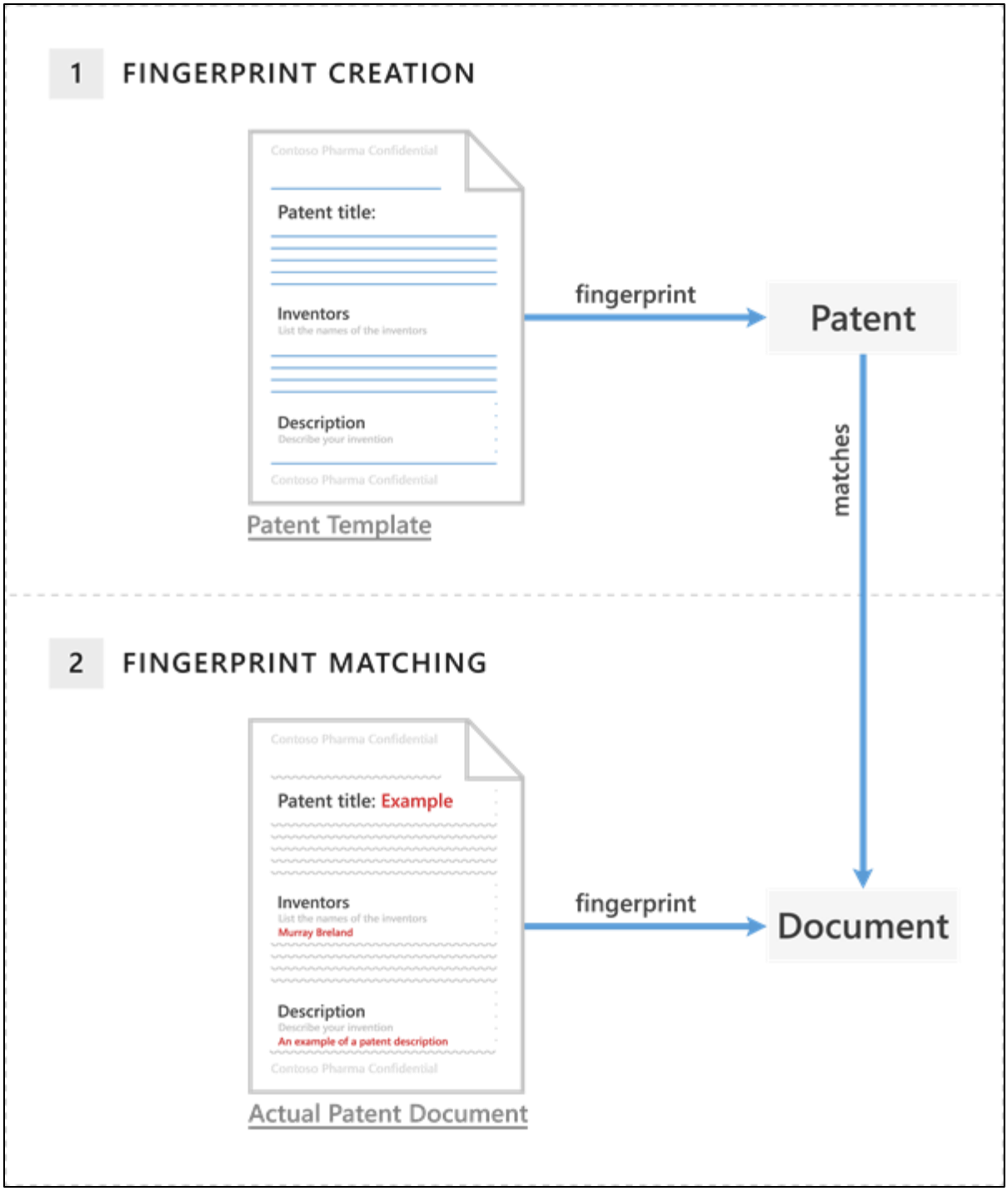
Configuring a document fingerprint as a custom sensitive information type allows you to prevent unintended sharing of documents created from official company templates. For example, human resources documents, possibly containing personal information, or patent documents containing intellectual property may be identified by document fingerprinting even if the content does not meet other sensitive information type criteria.

You've probably already guessed that documents don't have actual fingerprints, but the name helps explain the feature. In the same way that a person's fingerprints have unique patterns, documents have unique word patterns. When you upload a file, DLP identifies the unique word pattern in the document, creates a document fingerprint based on that pattern, and uses that document fingerprint to detect outbound documents containing the same pattern.

That's why uploading a form or template creates the most effective type of document fingerprint. Everyone who fills out a form uses the same original set of words and then adds their own words to the document. If the outbound document isn't password protected and contains all the text from the original form, DLP can determine if the document matches the document fingerprint.

Document fingerprint only works with Exchange Online.

The following picture shows the basic functionality how document fingerprint functions.



In this example, the patent template document contains the blank fields "Patent title," "Inventors," and "Description" and descriptions for each of those fields, which is the word pattern. When the word pattern is converted into a document fingerprint, a small Unicode XML file with a unique hash value is generated, which represents the original text.

The fingerprint is also saved as a data classification in Active Directory, as a security measure, because the original document itself isn't stored on the service, but only the hash value is stored, and the original document can't be reconstructed from the hash value. The patent fingerprint then becomes a sensitive information type that can be associated with a policy and any outbound emails containing documents created from the template, that match the patent fingerprint, are detected.

Document Fingerprinting supports the same file types that are supported in mail flow rules, for which an overview can be found in the resources at the end of this module. Document fingerprinting won't detect sensitive information in the following cases:

- Password protected files.
- Documents that only contain images.
- Documents that don't contain all the text from the original form used to create the document fingerprint.

Neither mail flow rules nor Document Fingerprinting supports the .dotx file type, even if this is a common file type for Word documents.

1.4.6. Create keyword dictionary

Keyword dictionaries are an efficient way to manage large lists of words that are regularly subject to change. Although you can create keyword lists in sensitive information types, keyword lists are limited in size and require modifying XML to create or edit them. Keyword dictionaries provide simpler management of keywords and at a much larger scale, supporting up to 1 MB of terms after compression in the dictionary and support of any language.

The source for keyword dictionaries can be several kinds of cleartext files, such as .txt and .csv files. Configuration of keyword dictionaries can be completed from the Microsoft 365 Compliance Center and via the Security & Compliance Center PowerShell module.

1.4.6.1. Keyword dictionary creation best practices

Consider the following a best practice to create your initial source keyword dictionary:

1.4.6.1.1. For a school

you can get together with a class of students to find words and phrases you don't want in an education environment.

1.4.6.1.2. For companies

you can use various options to collect:

1. Collect typical words from some departments, using Microsoft Forms
2. Collaborate with some employees for example, from HR or legal to create a list of typical words.
3. Create an employee audit and create the list out of the outcome.
4. Remember that you can edit the list, so you can improve your results by revising them regularly.

1.4.6.2. Keyword dictionary management

After creating a new keyword dictionary and using it in a policy, the keywords can be modified in case your requirements have changed. For example, a keyword dictionary used to detect disease classifications in medical data or for other static keywords required for policies.

1.4.6.3. Keyword dictionary as a custom sensitive information type

Keyword dictionaries can be used in rule package definitions for a custom sensitive information type. They can be selected as sensitive information types when creating policies in the Microsoft 365 Compliance Center or via the Security & Compliance Center PowerShell module. When using the PowerShell module, the keyword dictionary must be specified with its ID.

1.4.7. Knowledge check

1.4.7.1. Check your knowledge

1.4.7.1.1. Question

1. Which is the best sensitive information type for a large list of custom keywords?

- A built-in sensitive information type.
- A Keyword List in a custom sensitive information type.
- A Keyword Dictionary.

1.4.7.1.1.1. Correct Answer

This answer is correct. A large number of keywords can be used best in a Keyword Dictionary.

1.4.7.1.1.2. Wrong Answer

- A built-in sensitive information type.

This answer is not correct. Built-in information types cannot be modified to include custom keywords.

- A Keyword List in a custom sensitive information type.

This answer is not correct. A Keyword List is defined in the .xml definition and not suitable for a very large number of keywords.

1.4.7.1.2. Question

2. Which of the following items enables you to prevent unintended sharing of documents created from official company templates?

- Keyword Dictionary
- Document Fingerprinting
- Proximity indicators

1.4.7.1.2.1. Correct Answer

- Document Fingerprinting

This answer is correct.

1.4.7.1.2.2. Wrong Answer

- Keyword Dictionary

This answer is not correct.

- Proximity indicators

This answer is not correct.

1.4.7.1.3. Question

3. Which component of sensitive information types uses more evidence to reduce false positives?

- Character proximity
- Primary pattern
- Confidence level

1.4.7.1.3.1. Correct Answer

- Confidence level

This answer is correct.

1.4.7.1.3.2. Wrong Answer

- Character proximity

This answer is not correct.

- Primary pattern

This answer is not correct.

1.5. Understand Microsoft 365 encryption

1.5.1. Introduction to Microsoft 365 encryption

Encryption is the process of encoding information in a way that only authorized parties can read it. Using encryption protects data against theft, failures in physical security, and eavesdropping on data-in-transit. Most encryption methods use one or more keys. These keys provide the ability to read data that has been made unintelligible by encryption. Keys can be used to encrypt data, decrypt data, or both.

Encryption is an important part of the Microsoft data protection strategy and provides one layer of our Defense-In-Depth approach to security. Encryption contributes to data security and data privacy by providing an additional layer of defense against unauthorized disclosure of data. Encryption can also help meet compliance obligations or internal requirements to protect the confidentiality of sensitive or otherwise protected data.

Encrypting information renders it unreadable to unauthorized persons who manage to bypass other security controls. Even if an adversary were able to break through firewalls, infiltrate the network, obtain physical access to devices, or bypass permissions on a local

machine, the data in our systems would remain protected by strong encryption. A malicious attacker who obtained encrypted data without the appropriate key would be unable to decrypt and read the stolen data.

With Microsoft 365, multiple layers of encryption work together to secure customer data both at-rest and in-transit.

Customer data is encrypted at rest and in transit using FIPS 140-2 compatible encryption algorithms and technologies, including BitLocker, service encryption, Transport Layer Security (TLS), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES) algorithms. In addition, Microsoft employs advanced key management solutions to ensure that encryption keys are properly secured. This module will explore how each of these technologies is used in Microsoft 365, beginning with disk protection using BitLocker, followed by application-level protection with service encryption, and concluding with data-in-transit encryption implemented throughout Microsoft 365.

1.5.1.1. Examples of data-at-rest

include files uploaded to a SharePoint library, Teams chat messages, documents uploaded in Microsoft Teams meetings, email messages and attachments stored in mailbox folders, and files uploaded to OneDrive for Business.

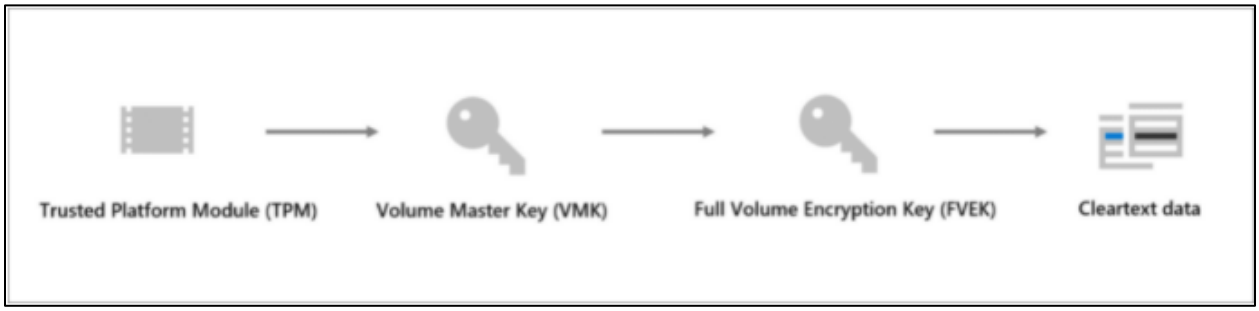
1.5.1.2. Examples of data-in-transit

include email messages that are in the process of being delivered or conversations that are taking place in an online meeting. In Microsoft 365, data is in transit whenever a user's device is communicating with a Microsoft server, or when Microsoft servers are communicating with one another.

1.5.2. Learn how BitLocker encrypts data-at-rest

Microsoft 365 uses BitLocker to encrypt the disk drives containing customer data at the volume level, ensuring all data-at-rest is encrypted. BitLocker encryption is a data protection feature built into Windows that integrates with the operating system and mitigates the threat of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. BitLocker is one of the technologies Microsoft 365 uses to safeguard data if lapses in other processes or controls (e.g., access control or recycling of hardware) were to lead to unauthorized physical access to disks containing sensitive data.

BitLocker is deployed with Advanced Encryption Standard (AES) 256-bit encryption on disks containing customer data. Disk sectors are encrypted with a Full Volume Encryption Key (FVEK), which is itself encrypted with the Volume Master Key (VMK), which in turn is bound to the Trusted Platform Module (TPM) in the server. Because the VMK directly protects the FVEK, protecting the VMK using the TPM is critical for preventing unauthorized access to the FVEK. BitLocker uses FIPS-compatible algorithms to ensure that encryption keys are not stored or sent over the wire in the clear. The Microsoft 365 implementation of customer data-at-rest-protection does not deviate from the default BitLocker implementation.



BitLocker key management protects recovery keys that are used to unlock and recover encrypted disks in a Microsoft datacenter. Microsoft 365 stores the master keys in a secured share, only accessible by individuals who have been screened and approved. The credentials for the keys are stored in a secured repository for access control data (what we call a "secret store"), which requires a high level of elevation and management approvals to access using a Just-In-Time (JIT) access elevation tool.

1.5.2.1. BitLocker two management categories

1.5.2.1.1. BitLocker-managed keys

which are generally short-lived and tied to the lifetime of an operating system instance installed on a server or to a given disk. These keys are deleted and reset during server reinstallation or disk formatting.

1.5.2.1.2. BitLocker recovery keys

which are managed outside of BitLocker, are used for disk decryption. BitLocker uses recovery keys for the scenario in which an operating system is reinstalled, and encrypted data disks already exist. Recovery keys are also used by Managed Availability monitoring probes in Exchange Online where a responder may need to unlock a disk.

1.5.3. Understand service encryption in Microsoft 365

In addition to using BitLocker for volume-level encryption, Microsoft 365 uses service encryption to encrypt customer data at the application layer.

Regardless of the selected key management option, the root keys are used to protect key hierarchies used by service encryption. All keys used for service encryption are stored securely in private repositories, such as Azure Key Vault, where they can be used by automated service code without direct accessibility by Microsoft personnel. Service encryption includes regular key rotation to maintain key security. Key rotation occurs through automated service code on internally defined schedules based on key type. Customers who use Customer Key are responsible for rotating their root Customer Keys based on their own security and compliance requirements.

Service encryption protects customer data with data encryption keys using one of the following key management options:

1.5.3.1. Key management options

1.5.3.1.1. Microsoft Managed Keys

In the default implementation for customers not using Customer Key, Microsoft manages all cryptographic keys used for service encryption. This option is currently enabled by default for Exchange Online, SharePoint Online, and OneDrive for Business. Microsoft Managed keys provide default service encryption unless a customer onboards to Customer Key.

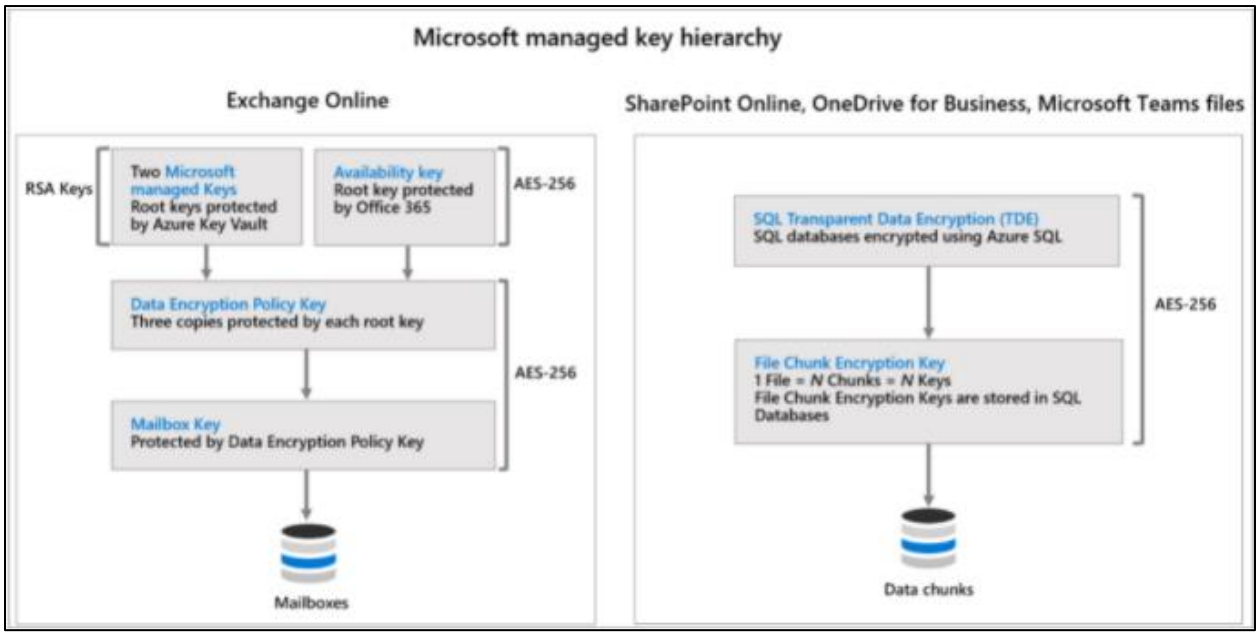
1.5.3.1.2. Customer Key

This option allows customers to use their own root keys to encrypt customer data. Customer keys are uploaded to or generated within Azure Key Vault, allowing customers to control the ability of Microsoft services to decrypt and process customer data. This option is currently available for Exchange Online, SharePoint Online, and OneDrive for Business.

1.5.3.2. Microsoft Managed Keys

With Microsoft Managed Keys, the Microsoft service manages and stores the root encryption keys used for service encryption, relieving the customer of the burden of provisioning and managing root encryption keys. Microsoft Managed Keys are stored in private key vaults that can only be accessed indirectly by Microsoft 365 services for data encryption. These keys cannot be accessed directly by Microsoft employees.

Microsoft Managed Keys are a viable solution for cloud customers that don't have key management requirements. For some customers, Microsoft Managed Keys may not meet their obligations for key management, operation, or storage. To meet these obligations, customer-managed keys can be implemented using the Customer Key feature.



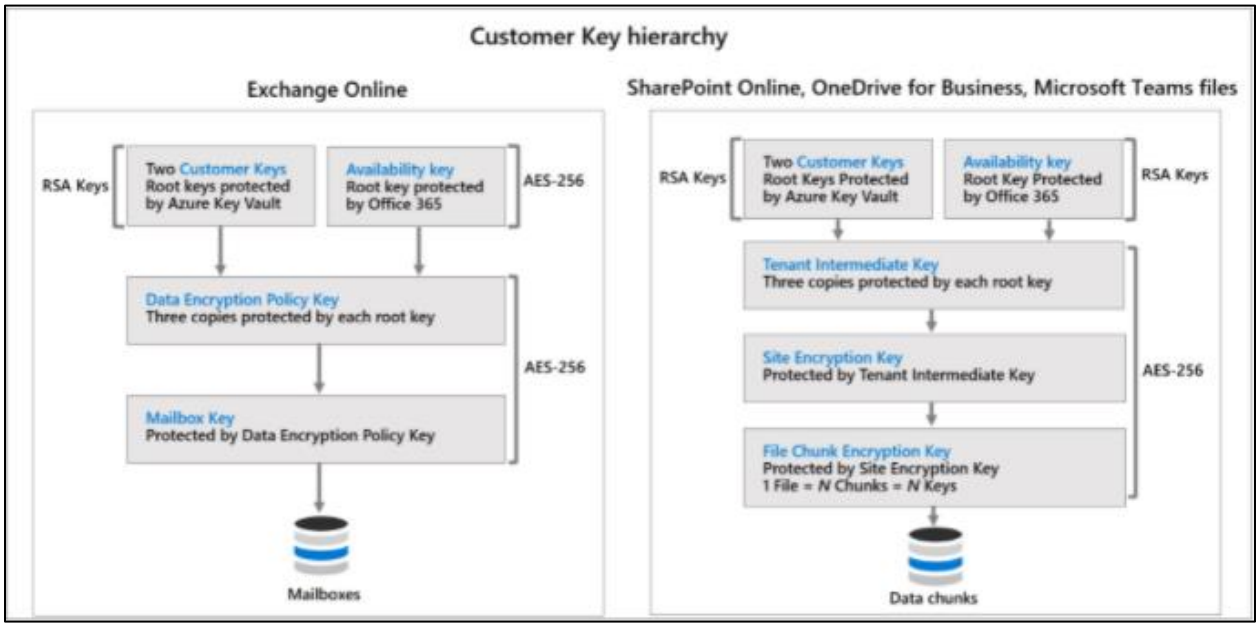
1.5.4. Explore customer key management using Customer Key

Customer Key is a feature that enables compliance with internal policies or external obligations involving the keys used for data encryption. These compliance obligations may include requirements to own the root keys used for data encryption, rotate keys on a defined cadence, or store keys in an HSM. Customer Key also provides customers the option to revoke their root keys and request a data purge when they leave the service, which shortens the time their data is retained in the cloud after service termination by cryptographically shredding the data, as outlined in the Online Services Terms

When using Customer Key, the customer's root keys leverage FIPS 140-2 compatible algorithms and do not leave the HSM boundary. As a result, customers may exercise their control and revoke their keys should they decide to exit the service. Revoking the keys and requesting a data purge renders encrypted data unreadable to our services.

The benefits of using Customer Key include:

- Providing rights protection and management features on top of strong encryption protection.
- Enhancing the ability of Microsoft 365 to meet the demands of customers with compliance requirements regarding encryption.



1.5.4.1. Availability key

For customers who use the Customer Key feature, Microsoft 365 provides data recovery capabilities using availability keys. The primary purpose of the availability key is to provide recovery capability from the unanticipated loss of customer-managed root keys, including key loss from mismanagement or malicious action. If customers lose control of their root keys, Microsoft Support can initiate recovery at the customer's request using the availability key.

The availability key is a root key provisioned and protected by Microsoft, which is functionally equivalent to the root keys supplied by the customer using the Customer Key feature. The availability key is automatically generated and provisioned when customers create a data encryption policy. By design, no one at Microsoft has access to the availability key: it is only accessible by Microsoft 365 service code. Microsoft 365 stores and protects the availability key, and unlike the keys that customers provide and manage in Azure Key Vault, customers cannot directly access the availability key. Nevertheless, Microsoft provides customers with sole authority over the disablement or destruction of the availability key. Should the customer decide to exit the service, the availability key is purged as part of the data purge process.

In addition to data recovery, the availability key is sometimes used to maintain service availability in Exchange Online. Although service failures are rare, transient Azure Active Directory or network issues can threaten the availability of Exchange Online content. If Exchange Online cannot reach the customer's root keys and we do not receive a response that indicates the customer has intended to block access to their root keys, the service falls back to the availability key to complete the operation. This rule only applies to Exchange Online. SharePoint Online and Microsoft Teams do not use the availability key unless the customer explicitly instructs Microsoft to initiate the recovery process.

Microsoft protects availability keys in access-controlled, internal secret stores, similar to the customer-facing Azure Key Vault. Access controls prevent unauthorized access to secret store contents. Secret Store operations, including key rotation and deletion, occur through automated commands that do not involve direct access to the availability key. Secret store management operations are limited to specific engineers and require privilege escalation through Lockbox. Privilege escalation requires manager approval and justification before access can be granted. Lockbox ensures access is time bound with automatic access revocation when the time period expires.

1.5.5. Learn how data is encrypted in-transit

In addition to protecting customer data-at-rest, Microsoft uses encryption technologies to protect customer data-in-transit. Data-in-transit scenarios include:

- When a client machine communicates with a Microsoft server.
- When a Microsoft server communicates with another Microsoft server.
- When a Microsoft server communicates with a non-Microsoft server (for example, Exchange Online delivering email to a third-party email server).

Inter-datacenter communications between Microsoft servers take place using TLS or IPsec, and all customer-facing servers negotiate a secure session using TLS with client machines. For example, client connections to Exchange Online use TLS with AES and FIPS 140-2 compatible implementations. This applies to the web protocols used by all clients, including Outlook, Microsoft Teams, and Outlook on the web.

Microsoft owns and manages its own certificate authority to manage the certificates used for TLS encryption alongside third-party solutions. The public certificates are issued by Microsoft using SSLAdmin, an internal Microsoft tool to protect confidentiality of transmitted information. All certificates issued by Microsoft IT have a minimum length of 2048 bits. Any certificates that fail to meet certificate provisioning criteria must be reviewed using a standardized exception process.

Customers can validate Microsoft's TLS configurations by going to Qualys SSL Labs and searching for the addresses of our public web portals.

1.5.6. Summary and knowledge check

In this module, you learned about how Microsoft 365 encrypts data-at-rest and in-transit, securely manages encryption keys, and provides key management options to customers to meet their business needs and compliance obligations.

Now that you have completed this module, you should be able to:

- Explain how encryption mitigates the risk of unauthorized data disclosure.
- Describe Microsoft data-at-rest and data-in-transit encryption solutions.
- Explain how Microsoft 365 implements service encryption to protect customer data at the application layer.
- Understand the differences between Microsoft managed keys and customer-managed keys for use with service encryption.

1.5.6.1. Check your knowledge

1.5.6.1.1. Question

1. Which of the following is a benefit of encryption?

- It is always legally required.
- It helps mitigate the impact of data theft.
- It renders data permanently unreadable.
- It meets all access control requirements.

1.5.6.1.1.1. Correct Answer

- It helps mitigate the impact of data theft.

Correct. When data is encrypted with strong encryption, it cannot reasonably be deciphered without the correct encryption key.

1.5.6.1.1.2. Wrong Answer

- It is always legally required.

Encryption requirements vary across data types and industries.

- It renders data permanently unreadable.

Encryption is a two-way process. Anyone with the correct encryption key can decipher encrypted data, making key management an important part of implementing strong encryption.

- It meets all access control requirements.

Encryption is not a substitute for access control.

1.5.6.1.2. Question

2. If a customer has stringent encryption requirements for key management that mandate keys are rolled every year, which of the following Microsoft 365 features should the customer use?

- Microsoft Managed Keys
- Availability key
- Customer Key

1.5.6.1.2.1. Correct Answer

- Customer Key

Customer Key provides customers the ability to manage encryption keys, which includes key rolling and key revocation.

1.5.6.1.2.2. Wrong Answer

- Microsoft Managed Keys

For some customers, Microsoft Managed Keys may not meet their compliance obligations or internal security requirements.

- Availability key

The availability key is part of Customer Key but is not a separate offering.

1.5.6.1.3. Question

3. Which of the following statements is accurate?

- Files sent between users in Microsoft 365 are encrypted using BitLocker.
- Microsoft 365 uses service encryption to encrypt customer data at the application layer.
- Microsoft utilizes a third party's certificate authority to manage all certificates used for TLS encryption.

1.5.6.1.3.1. Correct Answer

- Microsoft 365 uses service encryption to encrypt customer data at the application layer.

Correct. Additionally, Microsoft 365 encrypts data-at-rest using BitLocker.

1.5.6.1.3.2. Wrong Answer

- Files sent between users in Microsoft 365 are encrypted using BitLocker.

Microsoft 365 encrypts data-in-transit using TLS.

- Microsoft utilizes a third party's certificate authority to manage all certificates used for TLS encryption.

Microsoft owns and manages its own certificate authority to manage the certificates used for TLS encryption.

1.6. Deploy message encryption in Office 365

1.6.1. Introduction

Encryption is the system to restrict and control access to organizational data for different audiences. Understanding, configuring, and managing message encryption in Office 365 is an essential responsibility to keep internal and confidential intellectual property of organizations secret.

Encrypting organizational data, independent from target audiences who are granted access, is also a fundamental for many legal and regulatory requirements. Most organizations implement an encryption strategy only once in their tenant's lifetime, except when major legal or regulatory changes occur. Therefore, it is important to understand an organization's requirements for encryption.

By default, all newly created Microsoft 365 tenants use the Microsoft-generated keys for encryption. If the default key is sufficient for an organization's encryption strategy, there

are no further steps required for implementation of message encryption in Office 365. In this module, you will learn how implement message encryption in Office 365.

- Configure Office 365 Message Encryption for end users
- Implement Advanced Office 365 Message Encryption

1.6.2. Implement Office 365 message encryption

Once you have implemented your tenant encryption strategy, Office 365 Message Encryption can be implemented. To provide the best user experience, administrators should review their tenant settings for information rights management (IRM) features and OME settings before activating the encryption system for all users.

1.6.2.1. Verify information rights management functionality

Any Microsoft 365 tenant should be activated to use Azure RMS and IRM capabilities by default. To determine, if Azure RMS was deactivated for your tenant, run the following PowerShell cmdlets:

1. Run the following cmdlet to validate IRM configuration of a tenant:

```
Get-IRMConfiguration | fl AzureRMSLicensingEnabled
```

2. If the AzureRMSLicensingEnabled parameter is set to $False, activate OME for your tenant by using the following cmdlet:

```
Set-IRMConfiguration -AzureRMSLicensingEnabled:$True
```

3. Now run the following cmdlet with a sender inside your organization, to check if IRM data can be obtained for this recipient:

```
Test-IRMConfiguration -Sender admin@contoso.com -Recipient admin@contoso.com
```

4. The output of the cmdlet will display the results of several tests performed and an overall test result, which should be PASS.

The above cmdlets require a connection with the Exchange Online PowerShell and Exchange administrator permissions to change tenant-wide settings.

If any of the tests fail, you may not fetch the RMS templates for a recipient or there may be issues with the utilized encryption keys.

The IRM and OME configuration cmdlets allow you to configure how RMS content is used in a tenant and which key endpoints are in use. Administrators should become familiar with the available settings for these cmdlets.

1.6.2.2. Implement custom Office Message Encryption settings

OME is managed via configuration objects, or more precisely templates, which can be assigned and referenced. The default template for all users is named "OME Configuration" and any setting done in this configuration, is applied to all users. While the basic Office 365 Message Encryption allows only a single template, Office 365 Advanced Message Encryption provides more flexibility with multiple branding templates for different purposes.

The following examples provide a general description of which settings are available with the `*-OMEConfiguration` cmdlets and which settings should be configured when implementing OME for the first time. The first default template with the name "OME Configuration" is the default OME settings object for all users in a tenant.

If your tenant only includes Microsoft 365 E3 licenses, the number of cmdlets available is limited to managing the default OME template only. You cannot create new templates or add other Office 365 Advanced Message Encryption related settings.

1.6.2.3. OME branding templates

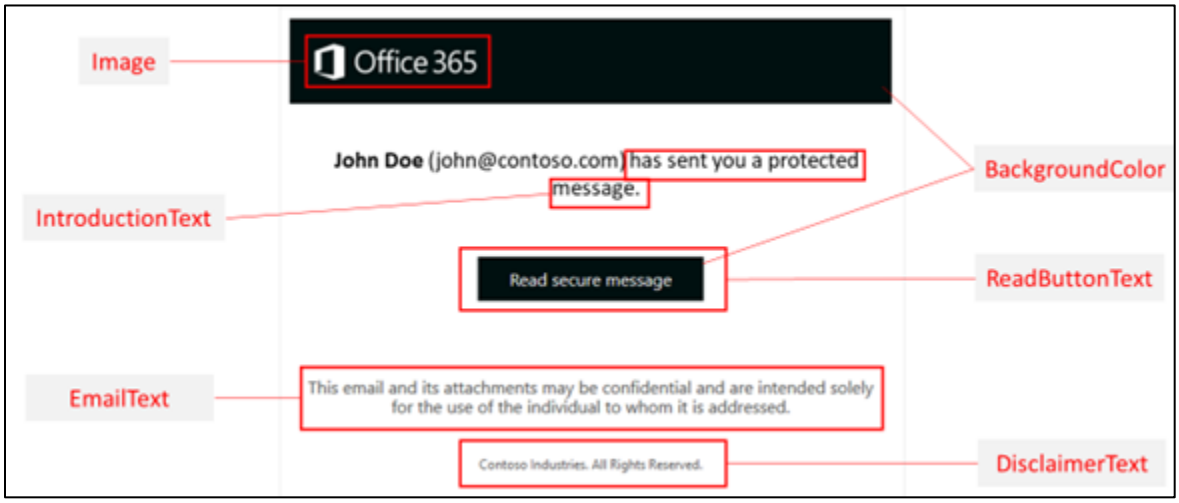
Customized company branding templates control the look of an organization's email messages and the encryption portal. The Get-OMEConfiguration and Set-OMEConfiguration Windows PowerShell cmdlets are used to modify the default template and to customize these parts of encrypted email messages:

1. Introductory text
2. Disclaimer text
3. URL for Your organization's privacy statement
4. Text in the OME portal
5. Logo that appears in the email message and OME portal, or whether to use a logo at all
6. Background color in the email message and OME portal

You can also revert to the default look and feel at any time.

Only Office 365 Advanced Message Encryption supports multiple templates

The following image provides an overview of the customizable areas of a branding template:



1.6.3. Implement Office 365 advanced message encryption

Office 365 Advanced Message Encryption allows you to use multiple templates for email messages and configure an expiration time for protected messages.

Use templates to fulfill several use cases, such as:

- Individual department templates, such as Finance, Sales, and so on.
- Templates for different geographical regions or countries
- If you want to allow emails to be revoked
- If you want emails sent to external recipients to expire after a specified number of days.

Once you've created the templates, you can apply them to encrypted emails by using Exchange mail flow rules. If you have Office 365 Advanced Message Encryption, you can revoke any email that you've branded by using these templates.

To create and remove new templates, the PowerShell cmdlets **New-OMEConfiguration** and **Remove-OMEConfiguration** are to be used.

1.6.3.1. Expiration date for email encrypted

You can use message expiration on emails that your users send to external recipients that use the OME portal to access encrypted emails. You can force recipients to use the OME portal to view and reply to encrypted emails sent from your organization by using a custom branded template that specifies an expiration date in Windows PowerShell.

You can only set expiration dates for emails to external recipients.

With Office 365 Advanced Message Encryption, anytime you apply custom branding, Office 365 applies the wrapper to email that fits the mail flow rule to which you have applied the template. In addition, you can only use expiration rules if you use custom branding.

Run the **New-OMEConfiguration** cmdlet, to create a new branding template with an expiration date of seven days:

```
New-OMEConfiguration -Identity "Expire in seven days" -ExternalMailExpiryInDays 7
```

ExternalMailExpiryInDays identifies the number of days that recipients can keep mail before it expires. You can use any value between 1–730 days.

1.6.4. Use Office message encryption templates in mail flow rules

The following example shows how to create mail flow rules to apply custom templates to email messages sent from your organization. Such a rule will apply custom branding, for example to senders from a specific department or members of a specific distribution group. You can also configure all mails from inside an organization to be encrypted when sent.

In the following example, you will configure a mail flow rule that encrypts all mails sent to the external partner organization Fabrikam, Inc., with the domain "fabrikam.com".

Perform the following steps to create a mail flow rule in the Exchange Admin Center (EAC):

1. In a web browser, navigate to the Exchange admin center at https://outlook.office365.com/ecp/.
2. Sign in using a work or school account that has been granted Exchange administrator permissions.
3. In the EAC, go to Mail flow > Rules and select **New ** > Apply Office 365 Message Encryption and rights protection to messages…
4. Enter the following information:
   4.1. In Name, type a name for the rule, such as Encrypt all mails to Fabrikam.
   4.2. In Apply this rule if…, select the condition The recipient address includes…, and any of these words.
   4.3. Enter fabrikam.com and select the plus (+) sign and Ok.

4.4. From Do the following..., select the Select one... text and from the RMS template list, Encrypt.
4.5. Select Save.

The list of templates includes default templates and options and any custom templates you create. If the list is empty, ensure that you have set up Office 365 Message Encryption with the new capabilities and IRM is activated for your tenant.

You can also perform this operation with Exchange Online PowerShell. If you use PowerShell you would not be using the RMS template named "Encrypt", but the OME Configuration name you want to configure instead. Use the following cmdlet to create a new mail flow rule to encrypt all messages sent to fabrikam.com:

```
New-TransportRule -Name "Encrypt all mails to Fabrikam" -FromScope InOrganization
-RecipientDomainIs "fabrikam.com" -ApplyRightsProtectionCustomizationTemplate
"OME Configuration"
```

1.6.5. Knowledge check

1.6.5.1. Question

1. How many templates does Office Message Encryption support?

- One
- Unlimited
- Five.

1.6.5.1.1. Correct Answer

- One

One is correct. Advanced Message Encryption is required to support more than one template.

1.6.5.1.2. Wrong Answer

- Unlimited

Unlimited is not correct. There is a limit.

- Five.

Five is not correct. The limit is not this high.

1.6.5.2. Question

2. What must be activated on your tenant before you can use Office Message Encryption?

- BitLocker
- Information Rights Management
- Microsoft 365 Compliance center

1.6.5.2.1. Correct Answer

- Information Rights Management

Information Rights Management is correct. You must have activate Information Rights Management to use Office Message Encryption

1.6.5.2.2. Wrong Answer

- BitLocker

BitLocker is not correct. BitLocker is not a requirement of Office Message Encryption.

- Microsoft 365 Compliance center

Microsoft 365 Compliance center is not correct. The Compliance center is not a requirement of Office Message Encryption.

1.6.5.3. Question

3. Which solution is the technology behind Office Message Encryption?

- Azure RMS.
- Service Encryption.
- BitLocker.

1.6.5.3.1. Correct Answer

- Azure RMS.

Azure RMS is correct. Azure RMS and IRM functionality is the technology supporting OME functionality.

1.6.5.3.2. Wrong Answer

- Service Encryption.

Service Encryption is not correct. Service Encryption is the application or tenant layer in between an organizations data saved in Microsoft 365 and servers in Microsoft 365 datacenters.

- BitLocker.

BitLocker is not correct. BitLocker is required to encrypt data at rest in Microsoft datacenters and hard disks in Windows 10 devices.

1.7. Protect information in Microsoft 365

1.7.1. Information protection overview

With information protection and sensitivity labels, you can intelligently classify and help protect your sensitive content.

Sensitivity labels let you classify and protect your organization's data, while making sure users can be productive and collaborate effectively. A sensitivity label, when applied, can restrict access to content using encryption, add a mark to the document (like a watermark), or do nothing at all.

Sensitive information types help define how Microsoft 365 recognizes specific kinds of information, such as health service numbers and credit card numbers. Microsoft 365 includes many ready to use sensitive information types to use when creating sensitivity labels. Sensitive information types can also be used with the Azure Information Protection scanner to classify and protect files on-premises.

Please refer to the Microsoft 365 licensing guidance for security and compliance for additional information on the licensing requirements for this solution.

1.7.1.1. Customer scenarios

Here are some common scenarios that Microsoft's solution for information protection can address:

1. Classify content to generate usage reports for your sensitive content.
2. Enforce encryption on any document labeled as confidential.

1.7.1.2. Getting started with information protection

Sensitivity labels are used to classify and protect your content. The administrator creates each label and defines what it can do. The sensitivity label is published, via a sensitivity label policy, to the users and groups you want to use the label. Users classify emails and documents as they work on them. Microsoft 365 enforces the protection settings on the content based on the label applied. Sensitivity labels can also be automatically applied so users do not have to classify content themselves.

A way to get started with sensitivity labels is to classify content without using any protection settings. You can assign a classification to content like a stamp that persists and roams with the content as it's used and shared. You can use this classification to generate usage reports and see activity data for your sensitive content. You can choose to apply protection settings later once you confirm it is working as expected. Of course, you'll need to educate users on how to classify their content in whatever application they are using.

Consider publishing new sensitivity label policies to a small number of users first. You can incorporate the feedback you receive from the initial group, as you publish the policy more broadly.

1.7.2. Configure sensitivity labels

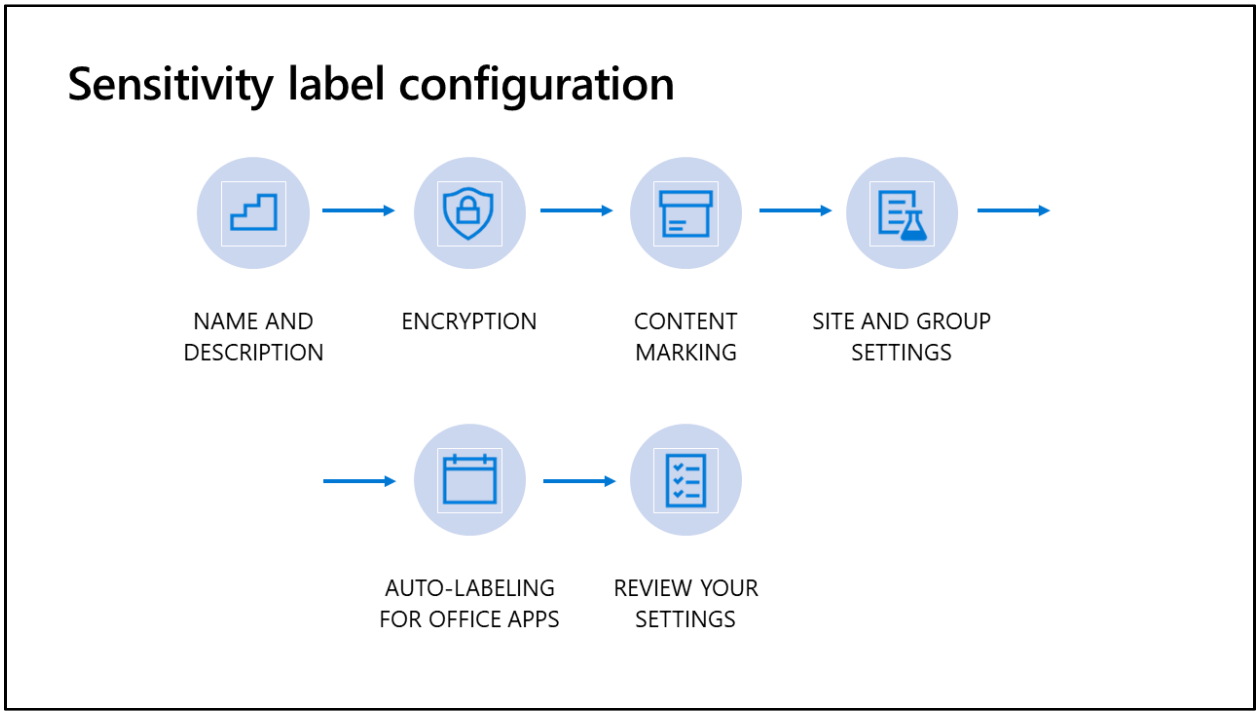
Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied, automatically or by the user, the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites.

The protection settings you choose for this label will be immediately enforced on the files, email messages or sites to which it is applied. Labeled files will be protected wherever they go, whether they are saved in the cloud or downloaded to a computer.

Here are the steps involved in sensitivity label configuration:

- Name and description
- Encryption
- Content marking
- Site and group settings (if preview enabled)

- Auto-labeling for Office apps
- Review your settings



1.7.2.1. Step 1: Name & Description

The step consists of providing the following information:

- Name
- Tooltip
- Description

1.7.2.1.1. Name

Enter a friendly name for the sensitivity label.

1.7.2.1.2. Tooltip

Enter text that helps users understand this label's purpose.

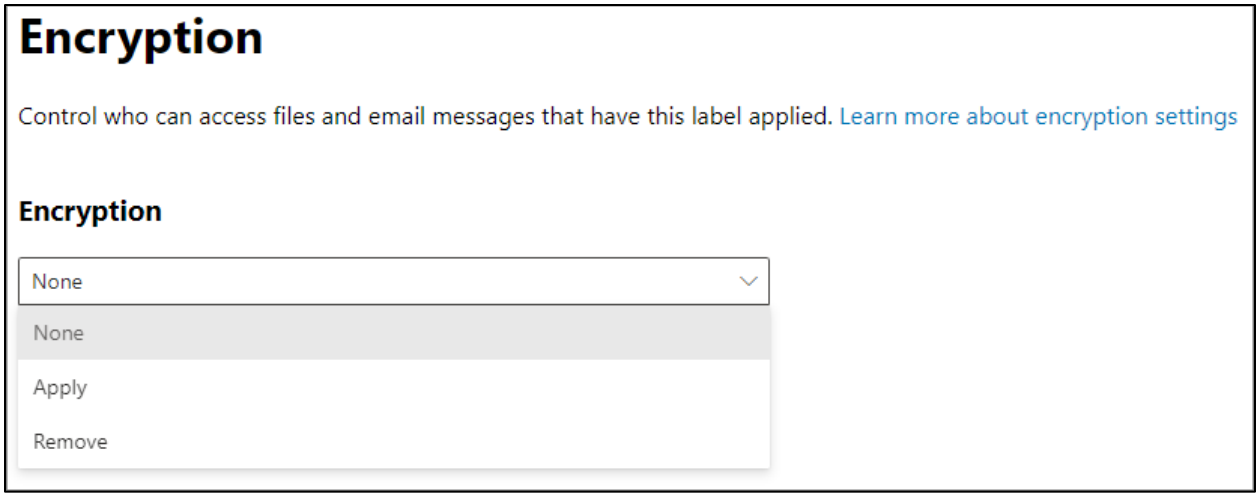
1.7.2.1.3. Description

Enter a description that's helpful for admins who manage this label. Adding the author and creation date are best practices.

1.7.2.2. Step 2: Encryption

The next step in the creation process is to determine who can access files and email messages that have this label applied. This is accomplished by configuring encryption settings. Encrypting your most sensitive documents and emails helps to ensure only authorized people can access this data. Encryption remains with the document wherever it goes and on whatever device it is accessed from. Encryption uses the Azure Rights Management Service (Azure RMS) from Azure Information Protection.

The image below shows the three encryption options: **None**, **Apply**, and **Remove**.



1.7.2.2.1. None

None means that original encryption is preserved for files and email messages with this label applied, however, if the label has administrator-defined permissions, the original encryption is removed.

1.7.2.2.2. Apply

Apply turns on encryption, which impacts Office files (Word, PowerPoint, Excel) with this label applied. Because the files will be encrypted for security reasons, performance will be slower when the files are opened or saved, and some SharePoint and OneDrive features may be limited or unavailable. The encryption settings you choose will be enforced when the label is applied to email and Office files.

1.7.2.2.2.1. Assign permission now or let users decide?

Choosing when to apply permissions is the next step in the process. Options are to assign them now let the users decide when they are going to apply them.

1.7.2.2.2.1.1. Assign permissions now.

Selecting this option means the encryption settings chosen will be enforced when the label is applied to email and Office files. Selecting this option results in the additional configuration choices shown below.

1.7.2.2.2.1.1.1. User access to content expires.

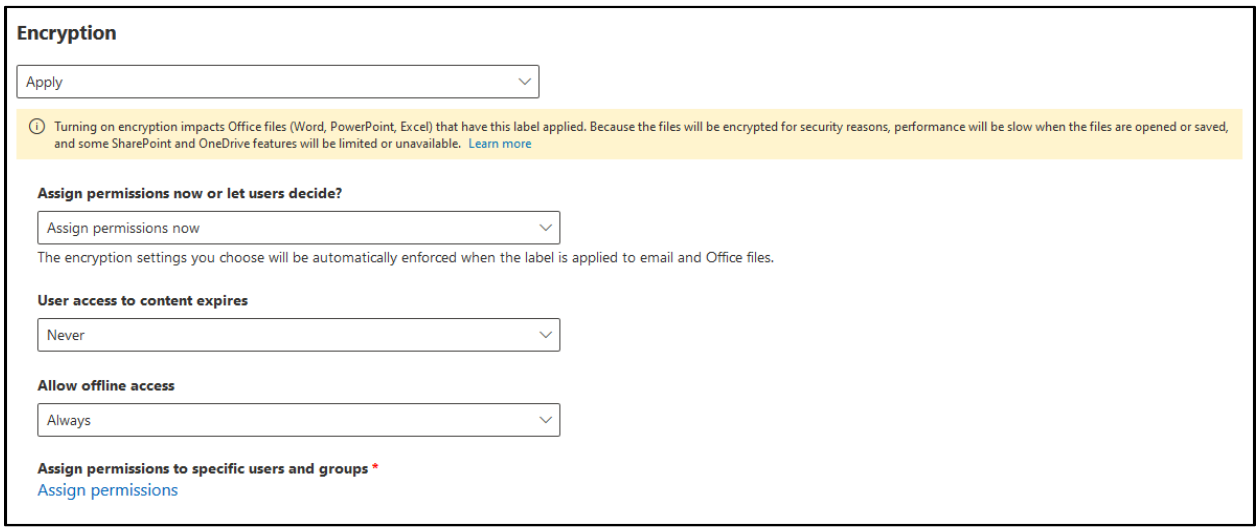
Options are never, on a specific date, and a number of days after the label is applied.

1.7.2.2.2.1.1.2. Allow offline access.

Options are never, on a specific date, and only for a number of days.

1.7.2.2.2.1.1.3. Assign permissions to specific users and groups.

Only the users or groups you choose will be assigned permissions to use the content with this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs. You must assign permissions to at least one user or group.



1.7.2.2.2.1.2. Let users assign permissions when they apply the label.

Selecting this option gives the user more control over what happens when the label is applied. These actions vary based on if the label is applied in Outlook or if it is applied in

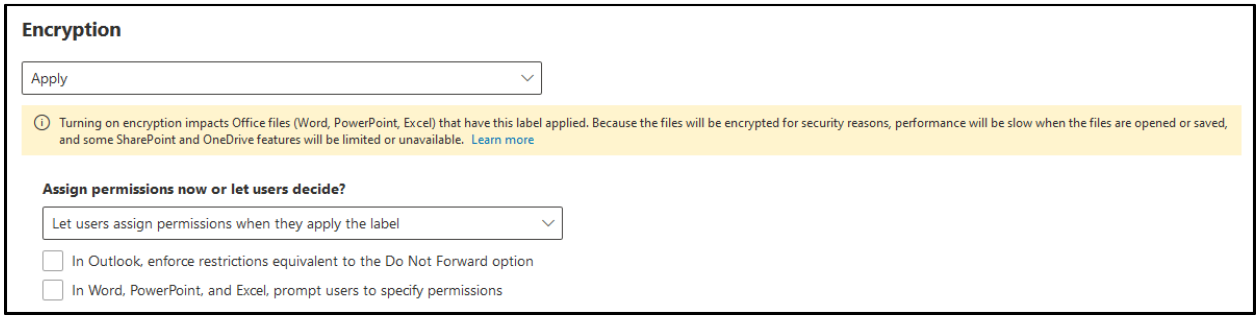
Word, PowerPoint, and Excel. Selecting this option results in the additional configuration choices shown below. You must choose at least one option.

1.7.2.2.2.1.2.1. Outlook.

The restrictions enforced are equivalent to the Do Not Forward option.

1.7.2.2.2.1.2.2. Word, PowerPoint, Excel.

The user will be prompted to specify permissions.



1.7.2.2.3. Remove

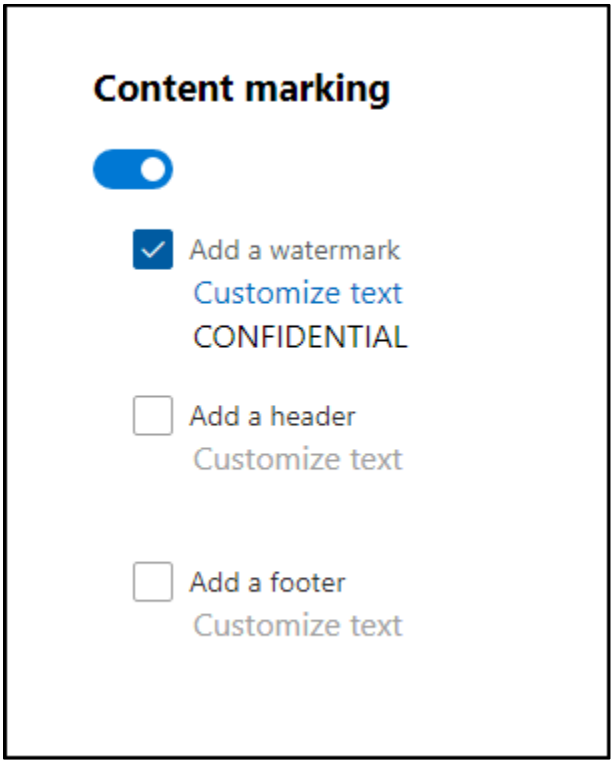
Remove means encryption will be removed on the files and email messages with this label applied.

1.7.2.3. Step 3: Content marking

Content marking adds custom headers, footers, and watermarks to email messages or documents when the label is applied. These marks are visible to the user. Content marking does not protect the document in any way. It only informs the viewer of the sensitive nature of the content. You can add one or more of the following text-only content marks:

- Watermark (documents only)
- Header
- Footer

Options to customize the text displayed include font size, font color and alignment.



1.7.2.4. Step 4: Site and group settings (preview)

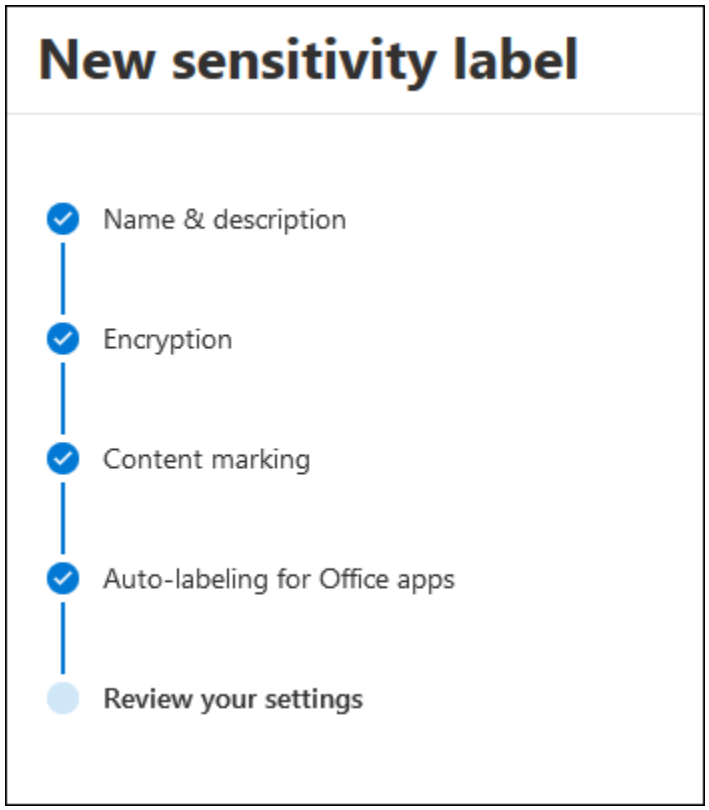
When you create sensitivity labels in the Microsoft 365 compliance center, you can now apply them to the following containers:

- Microsoft 365 groups
- SharePoint sites
- Microsoft Teams

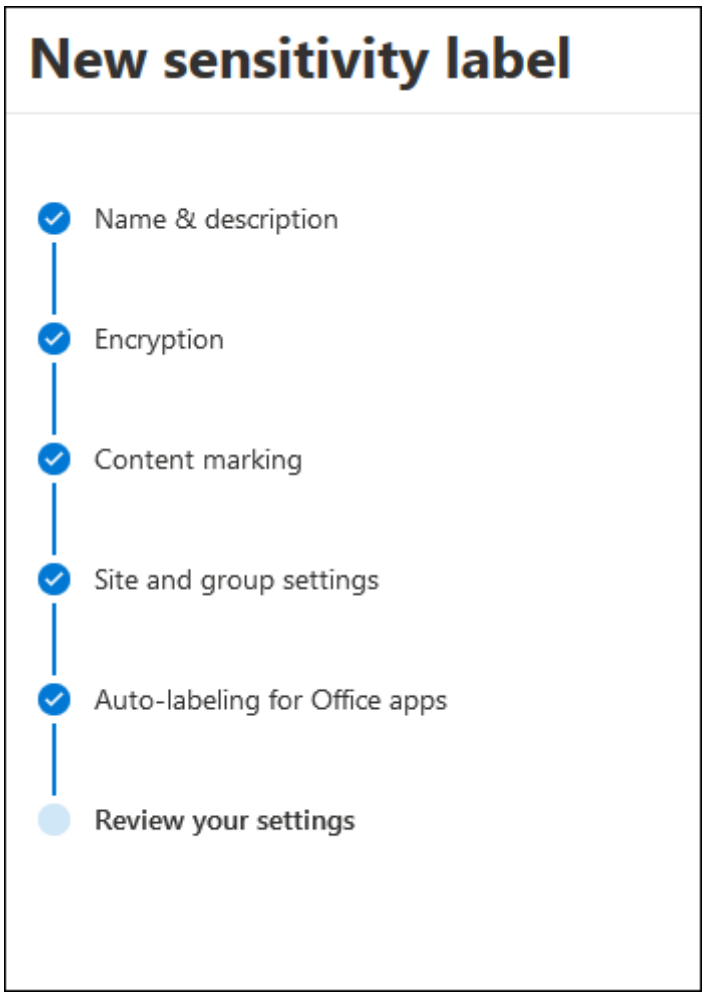
Content in the containers do not inherit the labels for settings such as the label name, visual markings, or encryption.

This page is only visible if the following preview is enabled: Use sensitivity labels with Microsoft Teams, Microsoft 365 groups and SharePoint sites. A link to more information is provided later in this unit.

The image below shows how the wizard appears if the preview feature has not been enabled.



This image below shows how the wizard appears if the preview feature has been enabled.



1.7.2.4.1. Privacy of Microsoft 365 group-connected team sites

Determine who can access a Microsoft 365 group or SharePoint site.

1.7.2.4.1.1. None

Let user choose who can access the site. Keep this default setting when you want to protect content in the container by using the sensitivity label, but still let users configure the privacy setting themselves.

1.7.2.4.1.2. Public

Anyone in the organization can access the site. Choose Public if you want anyone in your organization to access the team site or group.

1.7.2.4.1.3. Private

Only members can access the site. Chose Private if you want access to be restricted to only approved members in your organization.

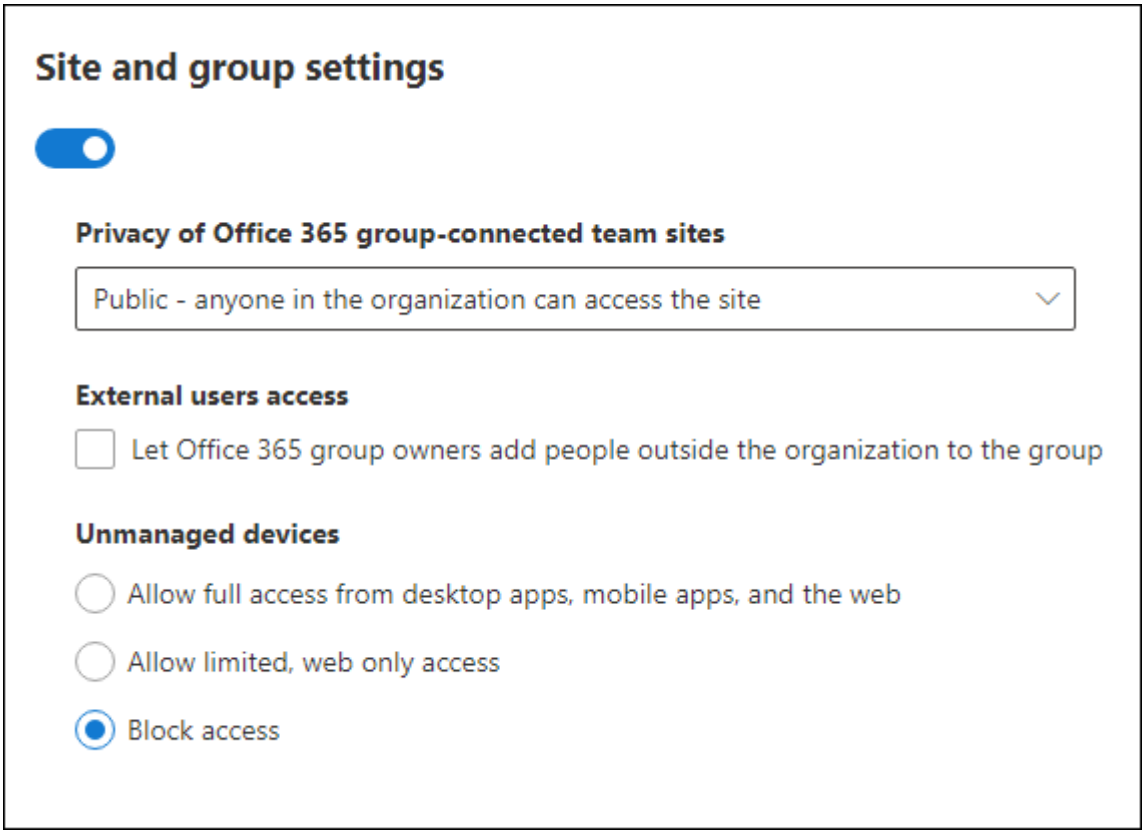
1.7.2.4.2. External users access

Control whether the group owner can add guests to the group.

1.7.2.4.3. Unmanaged devices

Specify the type of access users have from unmanaged devices. The options are:

- Allow full access from desktop apps, mobile apps and the web
- Allow limited, web only access
- Block access



1.7.2.5. Step 5: Auto-labeling for Office apps

When Microsoft 365 detects sensitive content in email or documents matching the conditions you specify, it can automatically apply the label or show a message to the user recommending they apply it themselves.

This feature is a capability included with

- Microsoft 365 E5
- Microsoft 365 E5 Compliance
- Microsoft 365 E5 Information Protection and Governance

Please review Microsoft 365 licensing guidance for security & compliance to identify required licenses for your organization.

1.7.2.5.1. Auto-labeling

1.7.2.5.1.1. Client-side auto-labeling

It is supported in Office apps on Windows for users who have either the Azure Information Protection unified labeling client or certain early adopter versions of Microsoft 365 Apps for enterprise (formally known as Office 365 ProPlus) installed.

1.7.2.5.1.2. Service-side labeling

It labels are applied to content already saved (in SharePoint Online or OneDrive) or emailed (processed by Exchange Online). In other words, these policies can automatically label files at rest and emails in transit based on the rules you've set. This method is sometimes referred to as auto classification with sensitivity labels. More information on service-side auto-labeling is available in the Automatic classification with sensitivity labels unit of this module.

1.7.2.5.2. Conditions

Under what conditions will auto-labeling be initiated? The conditions are defined using Sensitive information types and can vary in complexity. There can be a single condition or groups of conditions. You can also define the desired accuracy level of each sensitive information type and the number of instances it must have to become true.

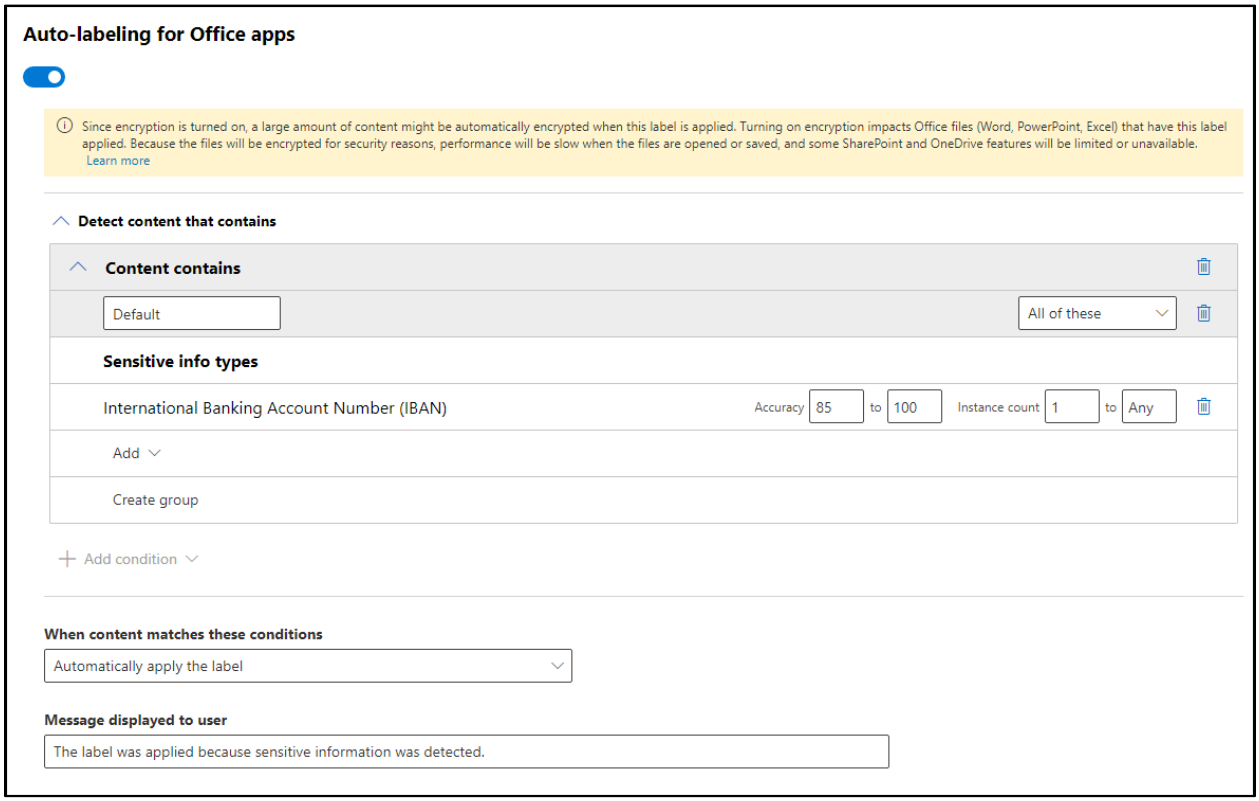
1.7.2.5.3. Action

What auto-label action should be taken when content matches the conditions? The two options available follow:

- Automatically apply the label
- Recommend the user apply the label

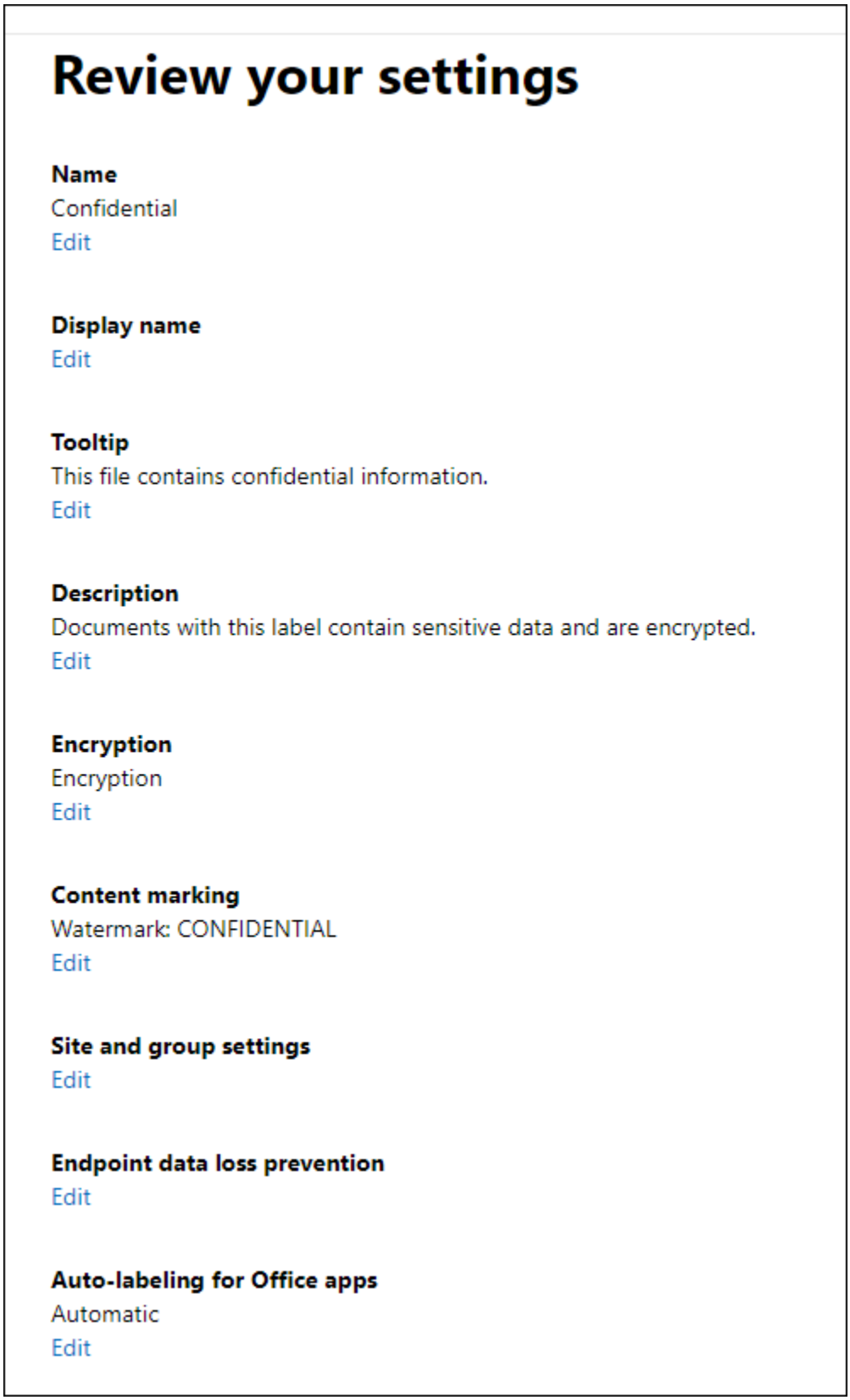
1.7.2.5.4. Message

What message should be displayed to the user informing them of the action?



1.7.2.6. Step 6: Review your settings

You will be given one last opportunity to review and edit your settings before submission. Hitting the submit button saves the label. It must be published or auto applied before it is enforced.



Review your settings

Name
Confidential
Edit

Display name
Edit

Tooltip
This file contains confidential information.
Edit

Description
Documents with this label contain sensitive data and are encrypted.
Edit

Encryption
Encryption
Edit

Content marking
Watermark: CONFIDENTIAL
Edit

Site and group settings
Edit

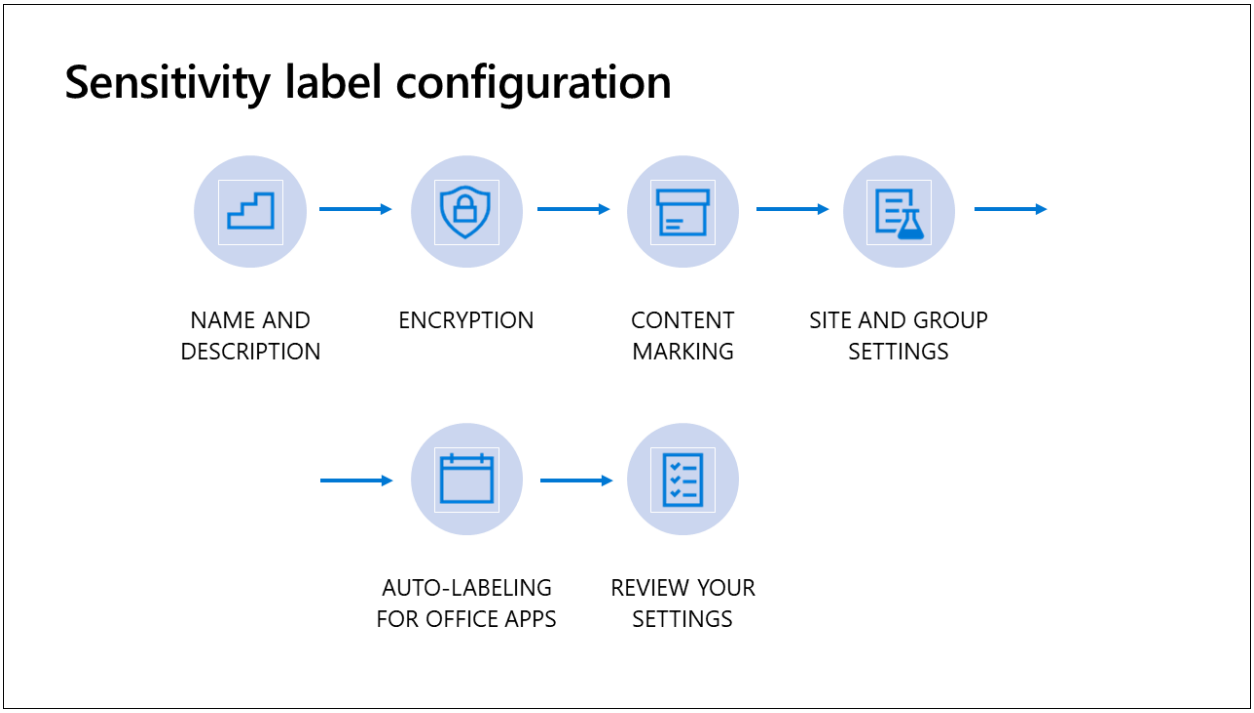
Endpoint data loss prevention
Edit

Auto-labeling for Office apps
Automatic
Edit

1.7.3. Configure sensitivity label policies

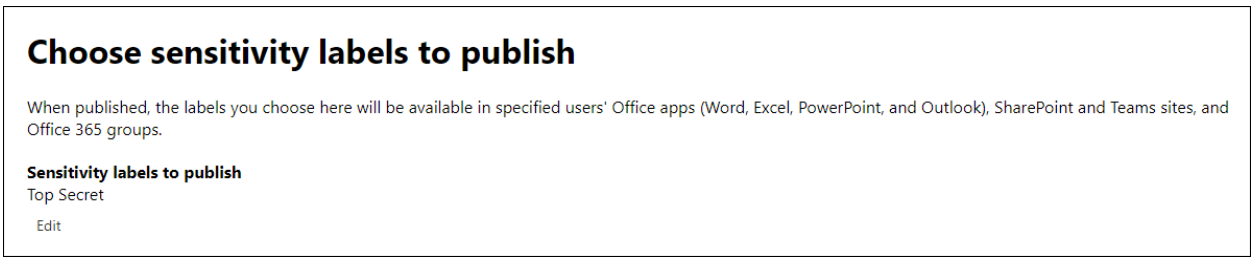
Creating a sensitivity label has no effect on users until it is published. You create sensitivity label policies to publish one or more labels to your Office apps (like Outlook and Word), SharePoint sites, Microsoft 365 groups, and Microsoft Teams. Once published, labels can be applied to protect their content. Here are the steps involved in sensitivity label policy configuration:

- Choose labels to publish
- Publish to users and groups
- Policy settings
- Name and description
- Review your settings



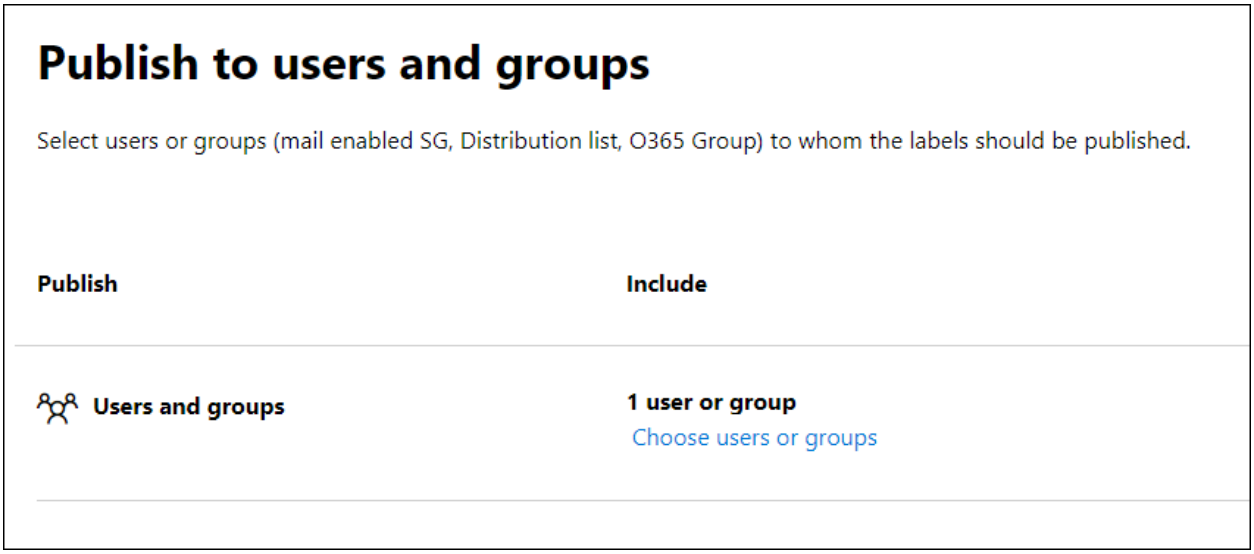
1.7.3.1. Step 1: Choose labels to publish

The first step is selecting one or more existing sensitivity labels to publish. The example below shows the sensitivity label **Top Secret** will be published with this policy.



1.7.3.2. Step 2: Publish to users and groups

This step involves choosing the users or groups to whom the labels should be published. This governs what users see the label, not where they see the label. The types of groups supported are email enabled-security groups, dynamic distribution groups, and Microsoft 365 Groups. Consider publishing the label to a test group with a few members first. You can add more groups to the policy once you validate it is working correctly.



1.7.3.3. Step 3: Policy settings

You can choose to have a default label, mandatory label, or require users to justify their actions.

1.7.3.3.1. Default label

You can select whether you want to apply a default label to documents and email. The options will be a combination of None and the labels you selected for publishing in the **Choose labels to publish** step.

1.7.3.3.2. Justification for removal

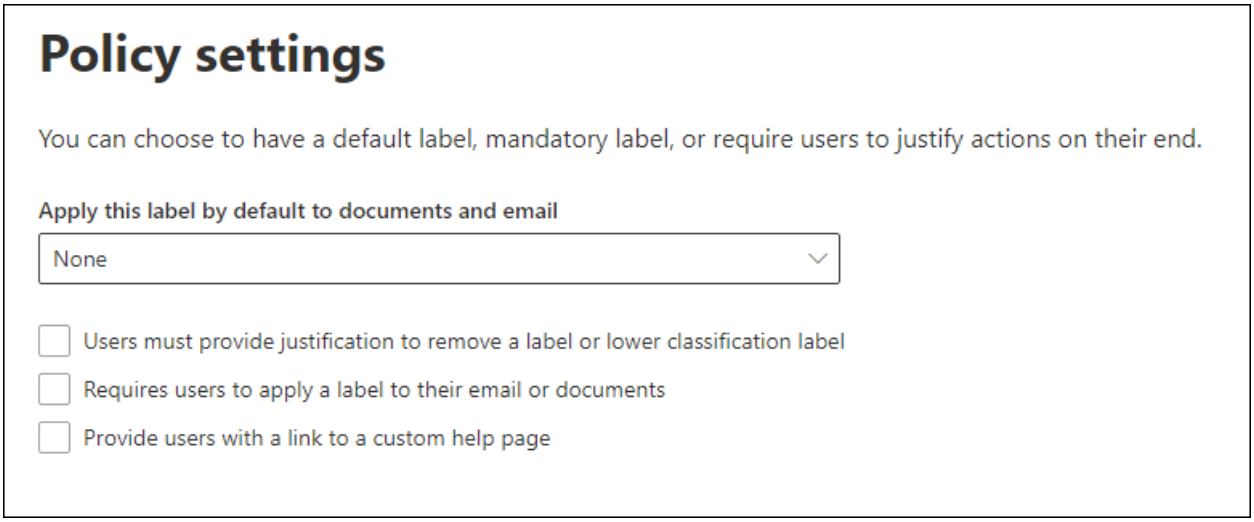
Selecting this option means the user will have to provide justification if a label is removed or if the classification is lowered. An example of lowering a classification might be changing the label from Confidential to Public. Label changes and removals are tracked in **Activity explorer.**

1.7.3.3.3. Require label

Selecting this option means users will be required to apply a label to their email or document, prior to sending or saving.

1.7.3.3.4. Custom help

Provide users with a link to a custom help page that provides additional information about the label policy. The admin would have to have the help content already created for this capability to work properly.



1.7.3.4. Step 4: Name and description

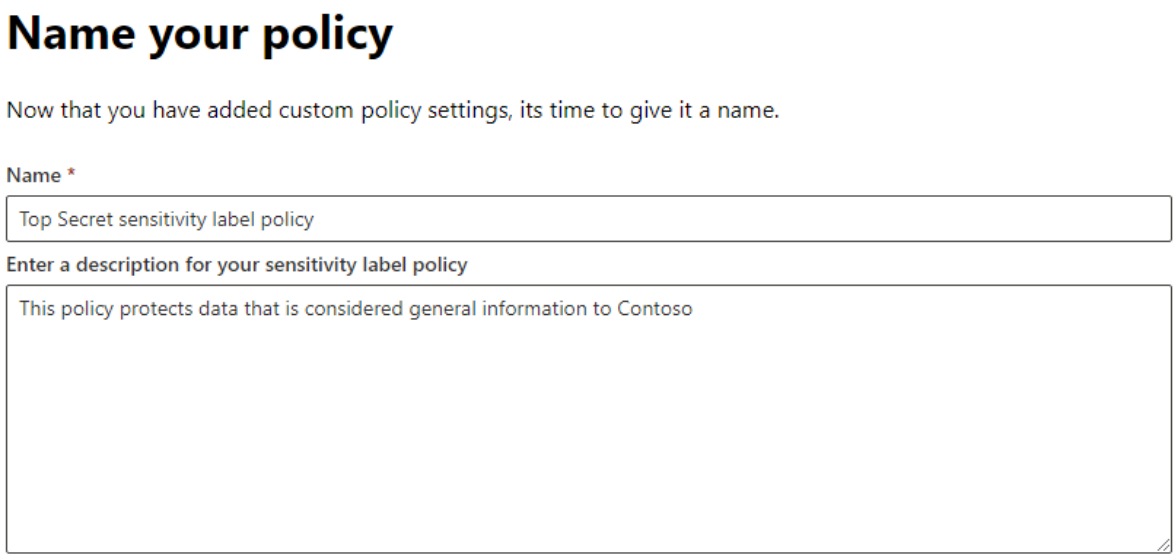
Now that you have added custom policy settings, it's time to give it a name.

1.7.3.4.1. Name

Enter a friendly name for the label policy.

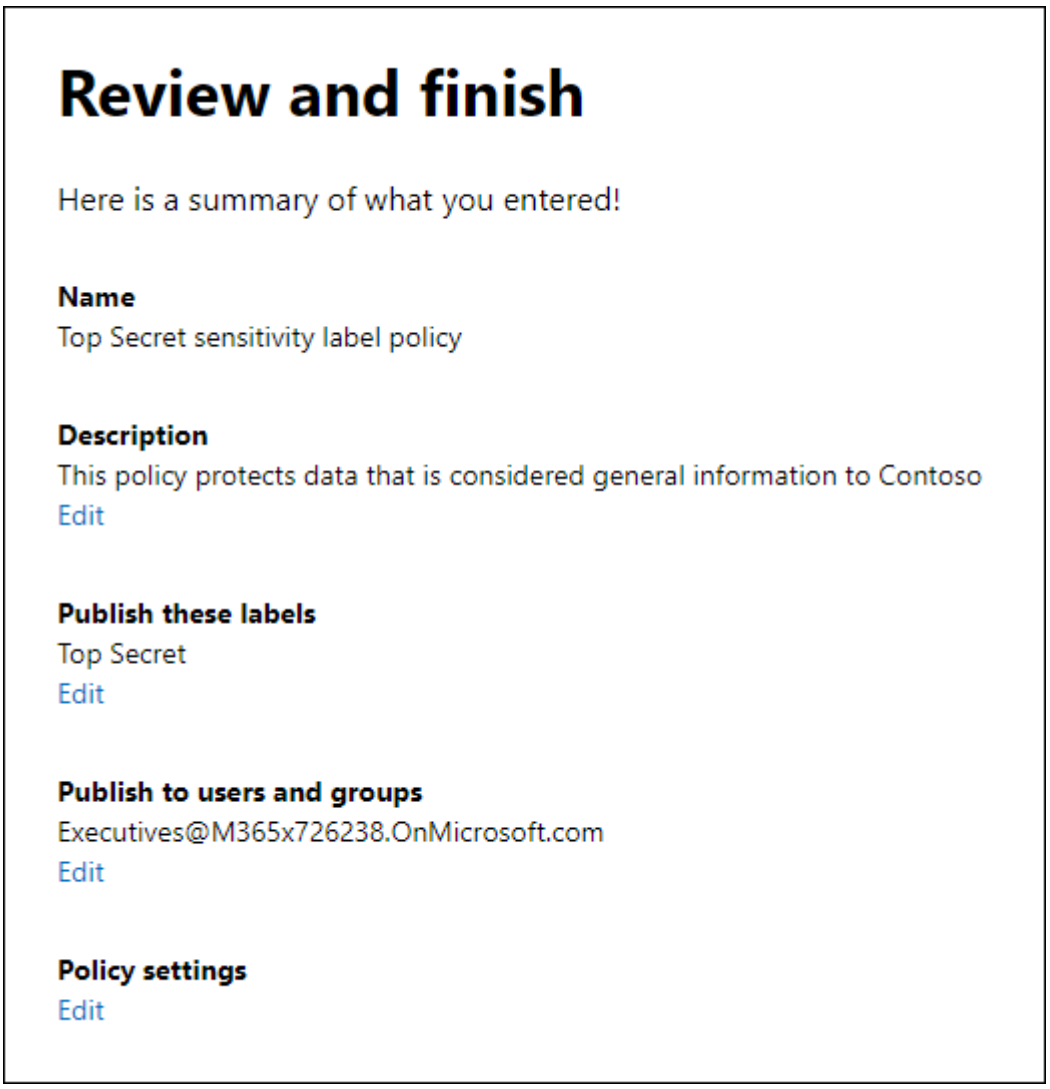
1.7.3.4.2. Description

Enter a description helpful for admins who manage this label policy.



1.7.3.5. Step 5: Review your settings

You will be given one last opportunity to review and edit your settings before submission. Submitting the label policy publishes the labels to the users and groups selected during this process.



1.7.4. Configure auto-labeling policies

You can now create auto-labeling policies to automatically apply sensitivity labels to email messages or documents that contain sensitive information stored in Microsoft 365 services like OneDrive, SharePoint Online, and Exchange Online. Because this labeling is applied by services rather than by applications, you don't need to worry about what apps users have and what version. As a result, this capability is immediately available throughout your organization and suitable for labeling at scale. These policies can automatically label files at rest and emails in transit based on the rules you set. Once created, policies will run in simulation mode to assist you in fine-tuning your auto-classification policy. Only after you are satisfied the policies are working as designed should you publish the label.

The steps to create an auto labeling policy are listed below:

- Info to label
- Name
- Choose locations
- Policy rules
- Label
- Policy mode
- Finish

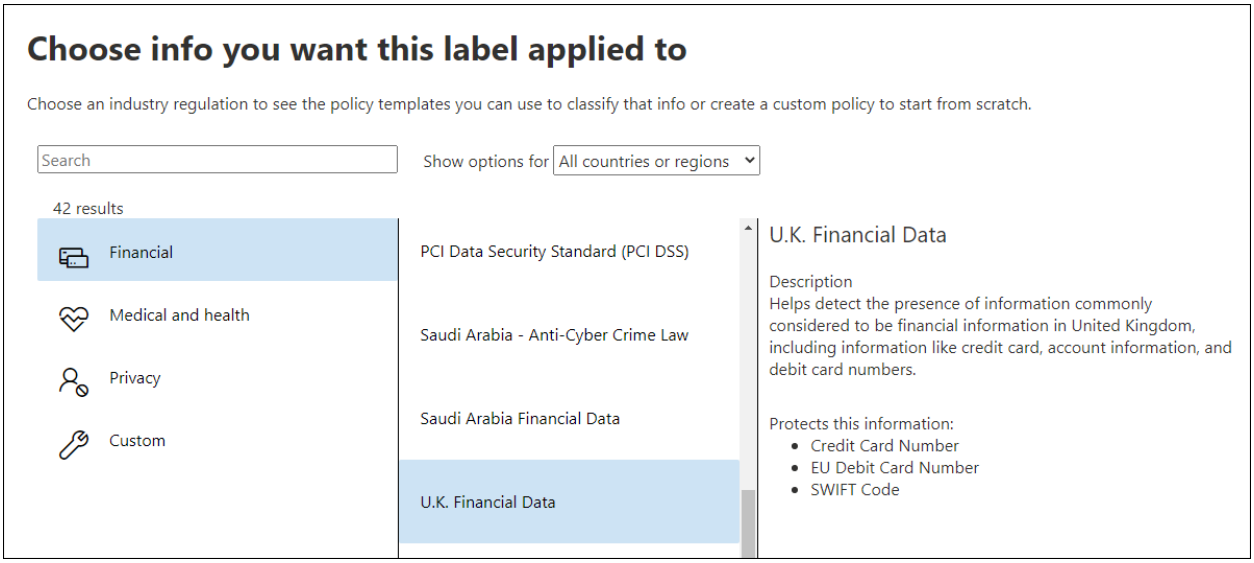
This feature is a capability included with:

- Microsoft 365 E5
- Microsoft 365 E5 Compliance
- Microsoft 365 E5 Information Protection and Governance

Please review Microsoft 365 licensing guidance for security & compliance to identify required licenses for your organization.

1.7.4.1. Step 1: Info to label

Start with a policy template or create a custom policy to choose the sensitive information you want this label applied to. Select a category to see the policy templates you can use or create a custom policy to start from scratch. If you need to protect labeled content, you will be able to choose labels later.



1.7.4.2. Step 2: Name

The next step is to give your policy a name and description.

1.7.4.2.1. Name

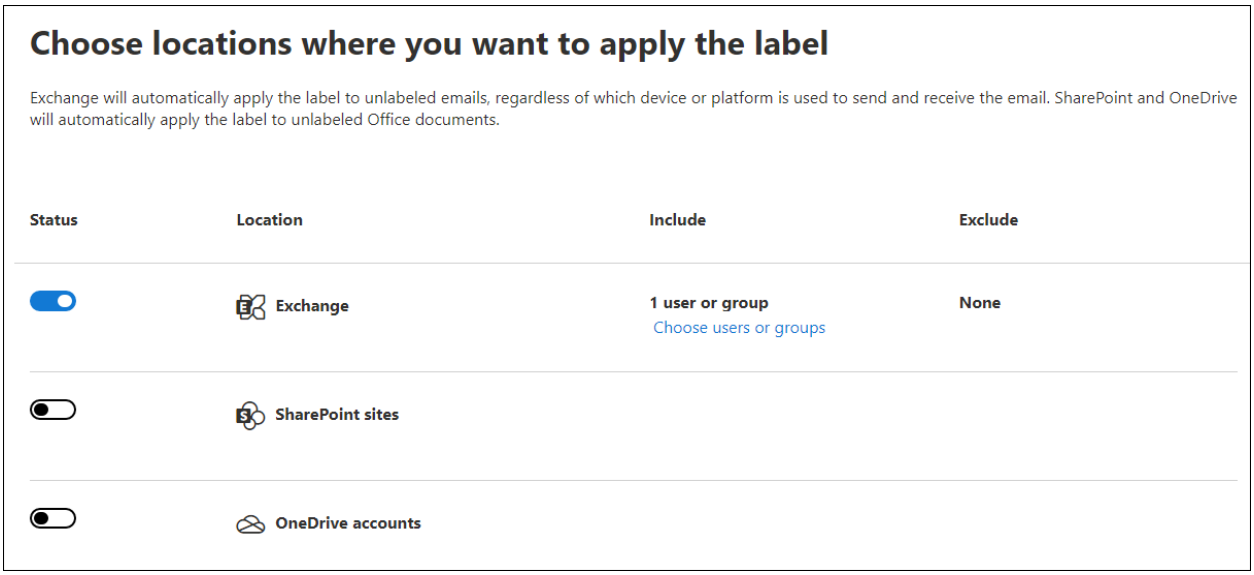
The name will be copied from the policy template, if selected in Step 1. It will be blank if the **Custom** option was selected.

1.7.4.2.2. Description

Provide information to help identify the automatically applied label, locations, and conditions that identify the content to label.

1.7.4.3. Step 3: Choose locations

Select which locations and users or groups (Exchange), sites (SharePoint), or accounts (OneDrive) the policy will apply to. Exchange will automatically apply the label to unlabeled emails, regardless of which device or platform is used to send and receive the email. SharePoint and OneDrive will automatically apply the label to unlabeled Office documents. The example below shows the configured policy will apply to one Exchange user or group and not SharePoint sites and OneDrive accounts. You can configure a maximum of 10 site collections in all auto-labeling policies at this time.



1.7.4.4. Step 4: Policy rules

The **Define policy settings** page has two options. Keep the default of **Find content that contains** to define rules that identify content to label across all your selected locations. If you need different rules per location, select **Advanced settings**.

The rules use conditions that can include sensitive information types and sharing options:

- For **Content contains sensitive info types**, you can select both built-in and custom sensitive information types.
- For the **Content is shared** option, you can choose **only with people inside my organization** or **with people outside my organization**.

If your only location is Exchange, or if you select **Advanced settings**, there are additional conditions that you can select. They include:

- Sender IP address is
- Recipient domain is
- Recipient is
- Attachment's file extension is
- Attachment is password protected
- Document property is
- Any email attachment's content could not be scanned
- Any email attachment's content didn't complete scanning

1.7.4.5. Step 5: Label

Choose a label to auto-apply. Users will see the selected sensitivity label applied to files that match the rules specified.

1.7.4.6. Step 6: Policy mode

Decide if you want to run the simulation now or wait until later.

1.7.4.6.1. Run policy in simulation mode

Running the policy in simulation mode before activation helps ensure the label is being applied to the correct items. You can do this right away or wait until later. Selecting this option starts the simulation.

1.7.4.6.2. Leave policy turned off

Selecting this option leaves the policy in an inactive state ready to run in simulation mode.

1.7.4.7. Step 7: Finish

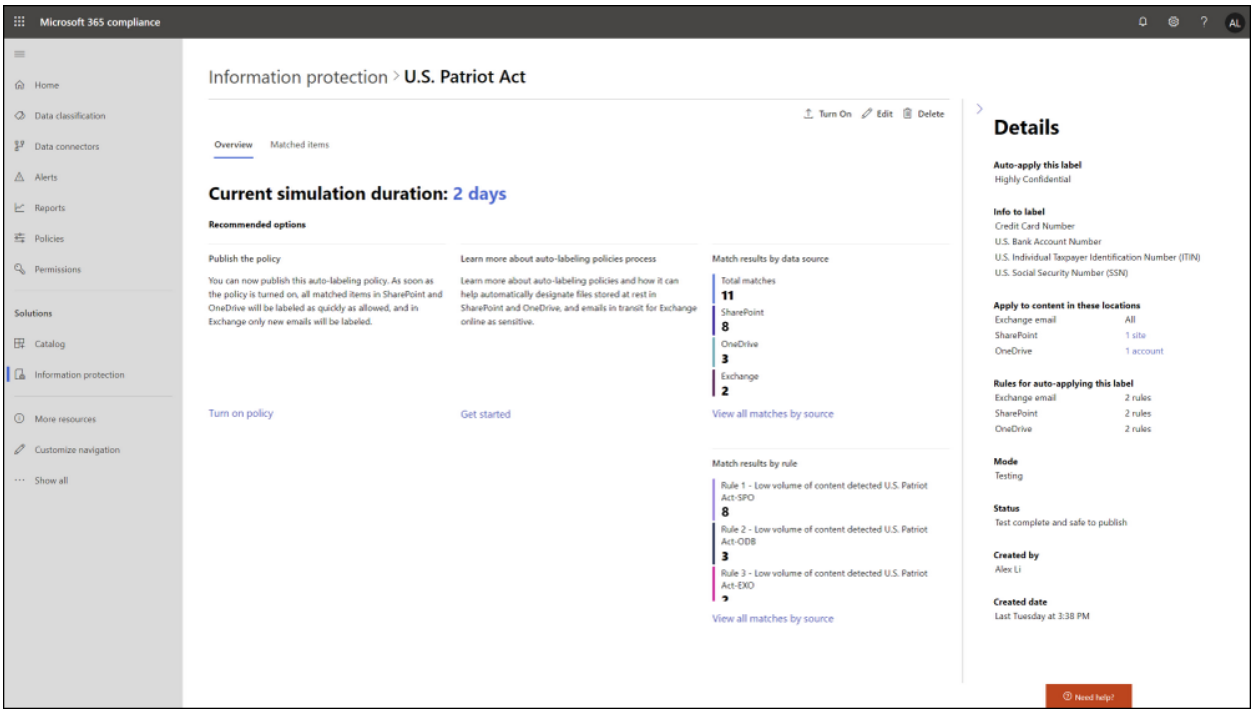
You will be given one last opportunity to review and edit your settings before submission. Unlike auto-labeling for Office apps, there's no separate publish option. Allow up to 24 hours for the auto-labeling policy to replicate throughout your organization.

1.7.4.7.1. Simulation mode

The **Policy Simulator** assists you in validating and fine-tuning your auto-labeling policies. You can validate your policies prior to enforcement. Policies can be published in successively broader scopes, thereby mitigating the risk of unintended consequences. Select an individual policy to see the details of the configuration and its status. **Policy Simulator** is designed to:

- Help you understand the impact of the policy and tune it for accuracy and scalability.
- Provide insights on the estimated length of time required to deploy a policy at scale.
- Prevent deployment of ineffective or bad policies and help minimize incident management costs.

The image below shows an auto-label policy named **U.S. Patriot Act** that has been running in simulation mode for two days. You can click on the **Matched items** tab to see the results of your auto-labeling policy simulation, provided you have the appropriate permissions. Selecting **Turn on policy** starts policy enforcement.



1.7.5. Manage, monitor, and remediate information protection

The **Data classification** solution provides information about your organization's data once it has been classified. It helps you identify exposure and risks to inform policies that help you protect and govern your data. It not only helps during the process of getting to know your data. It also helps you monitor the status of your classification work on an ongoing basis. It was already covered in this learning path, so we will review the parts of the solution relevant to protecting your data.

These cards from the **Overview** page are most relevant to information protection:

1. Top sensitive information types
2. Top sensitivity labels applied to content
3. Top activities detected
4. Locations where sensitivity labels are applied
5. Azure Information Protection labels summary

Each summary card except for **Azure Information protection labels summary** links to either **Activity explorer** or **Content explorer**, where you can examine the data more thoroughly.

1.7.6. Summary and knowledge check

In this module, you learn how to discover, classify, and protect sensitive and business-critical content throughout its lifecycle across your organization.

Now that you have completed this module, you should be able to:

- Discuss the information protection solution and its benefits.
- List the customer scenarios the information protection solution addresses.
- Describe the information protection configuration process.
- Explain what users will experience when the solution is implemented.
- Articulate deployment and adoption best practices.

1.7.6.1. Check your knowledge

1.7.6.1.1. Question

1. Which capability of Microsoft information protection defines health service numbers or credit card numbers by patterns?

- Sensitive information types
- Sensitivity labels
- Data loss prevention

1.7.6.1.1.1. Correct Answer

- Sensitive information types

Microsoft 365 includes many sensitive information types that are ready for you to use in DLP policies and for automatic classification with sensitivity and retention labels. Sensitive information types define how the automated process recognizes specific information types such as health service numbers and credit card numbers.

1.7.6.1.1.2. Wrong Answer

- Sensitivity labels

With sensitivity labels, you can classify and help protect your sensitive content. Protection options include labels, watermarks, and encryption.

- Data loss prevention

With DLP policies, you can identify, monitor, and automatically protect sensitive information across Office 365. Data loss prevention policies can use sensitivity labels and sensitive information types to identify sensitive information.

1.7.6.1.2. Question

2. Which of the following statements regarding encryption and sensitivity labeling configuration is accurate?

- Encryption prevents any chance of data loss internally or externally for the organization.
- When a sensitivity label is applied to existing encrypted permissions by a specified user and the encryption “None “ option is selected, the new label encryption is applied.
- Encryption remains with the document wherever it goes on whatever device.

1.7.6.1.2.1. Correct Answer

- Encryption remains with the document wherever it goes on whatever device.

The document remains encrypted no matter where it resides, inside or outside your organization, even if the file is renamed.

1.7.6.1.2.2. Wrong Answer

- When a sensitivity label is applied to existing encrypted permissions by a specified user and the encryption “None “ option is selected, the new label encryption is applied.

When a sensitivity label is applied to existing encrypted permissions by a specified user and encryption “None “ option is selected, the original encryption is preserved.

- Encryption prevents any chance of data loss internally or externally for the organization.

Encryption cannot prevent manual data loss such as a user taking a picture of the screen.

1.7.6.1.3. Question

3. When viewing your sensitivity labels list in the Information protection solution, the order of the labels is important because it reflects their priority. You want your most restrictive sensitivity label, such as Highly Confidential, to appear at the bottom of the list, and your least restrictive sensitivity label, such as Public, to appear at the top. What best practice should you implement if users in your organization typically try to remove labels or replace labels with lower order numbers?

- Apply a default label
- Remove the user
- Require justification

1.7.6.1.3.1. Correct Answer

- Require justification

If a user tries to remove a label or replace it with a label that has a lower-order number, you can require the user provides a justification to perform this action.

1.7.6.1.3.2. Wrong Answer

- Apply a default label

Consider using a default label to set a base level of protection settings that you want applied to all your content. However, without user training and other controls, this setting can also result in inaccurate labeling.

- Remove the user

If a user tries to remove a label or replace it with a label that has a lower-order number, you can require the user provides a justification to perform this action.

1.7.6.1.4. Question

4. How do you add custom headers or footers to email messages or documents when the label is applied?

- Encryption
- Content marking
- Auto-labeling

1.7.6.1.4.1. Correct Answer

- Content marking

Content marking adds custom headers, footers, and watermarks to email messages or documents when the label is applied. These marks are visible to the user. Content marking does not protect the document in any way.

1.7.6.1.4.2. Wrong Answer

- Encryption

Encrypting your most sensitive documents and emails helps to ensure only authorized people can access this data.

- Auto-labeling

When Microsoft 365 detects sensitive content in email or documents matching the conditions you specify, it can automatically apply the label or show a message to the user recommending they apply it themselves.

1.7.6.1.5. Question

5. You can create auto-labeling policies to automatically apply sensitivity labels to email messages or documents that contain sensitive information in OneDrive for Business. What feature of auto-labeling eliminates the worry about what apps users have or what version?

- Labeling is applied by services
- Labeling is applied by applications
- Labeling is applied manually

1.7.6.1.5.1. Correct Answer

- Labeling is applied by services

Because this labeling is applied by services rather than by applications, you don't need to worry about what apps users have and what version. As a result, this capability is immediately available throughout your organization and suitable for labeling at scale.

1.7.6.1.5.2. Wrong Answer

- Labeling is applied by applications

Because this labeling is applied by services rather than by applications, you don't need to worry about what apps users have and what version. As a result, this capability is immediately available throughout your organization and suitable for labeling at scale.

- Labeling is applied manually

Because this labeling is applied by services rather than by applications, you don't need to worry about what apps users have and what version. As a result, this capability is immediately available throughout your organization and suitable for labeling at scale.

1.8.Apply and manage sensitivity labels

1.8.1. Introduction

Once you have created sensitivity labels and configured label policies, you can start using them in your organization. In this module, you will learn how to manage sensitivity labels. You will also learn to apply sensitivity labels to emails and files.

After sensitivity labels are implemented and your organization has been using them for some time, you should evaluate their effectiveness and perhaps fine-tune label policies. Using Label Analytics you can identify which sensitivity labels trigger too many false positives. In this module, you will learn how to monitor sensitivity label performance using these tools.

Upon completion of this module, you should be able to:

- Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites.
- Monitor label usage using label analytics.
- Configure on-premises labeling.
- Manage protection settings and marking for applied sensitivity labels.
- Apply protections and restrictions to email and files.

1.8.2. Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites

You can apply sensitivity labels to Microsoft 365 Groups and SharePoint sites. This enables lifecycle management of content within different types of containers of Microsoft 365.

Containers where labels can be published include:

- Microsoft 365 Groups
- Microsoft Teams
- Yammer Communities
- SharePoint Sites

Possible restrictions to configure via sensitivity labels:

- Privacy option (Public/Private/None)
- External User Access (Allowed/Forbidden)
- Control external sharing from labeled SharePoint Sites (Anyone/New and existing guests/Existing guests/Only people of organization)
- Access from unmanaged devices (Allow full access/Allow limited, web-only access/Block access)

1.8.2.1. Options for applying a sensitivity label to groups and SharePoint sites

There are many ways to apply a label to a Group and SharePoint site.

- Creation wizard of a Group or SharePoint Site
- SharePoint Admin Center for existing ones
- Microsoft Teams Admin Center for existing ones
- Azure portal
- PowerShell

1.8.2.1.1. Applying labels to SharePoint Online & Microsoft 365 Groups

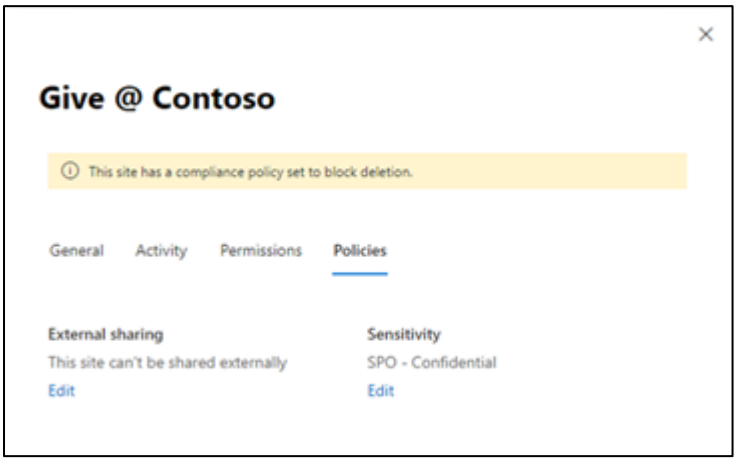
Sensitivity labels can be applied at different locations and via different applications.

1.8.2.1.2. SharePoint admin center

As a SharePoint administrator you can use the SharePoint Admin center to change or assign a sensitivity label to a SharePoint Site:

1. Navigate to the **Microsoft 365 admin center** at https://admin.microsoft.com/

2. Select **… Show all** and **SharePoint**.
3. Navigate to **Sites** > **Active Sites**.
4. Select the checkmark left of an existing site in which you want to apply a published Sensitivity Label to.
5. For the selected site, navigate to **Policies**.

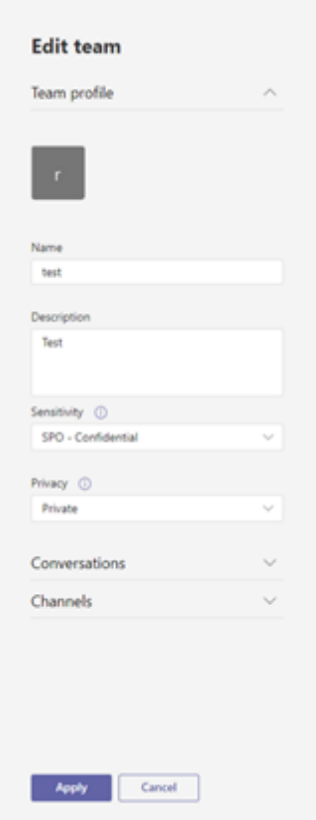


6. Select edit to set the Sensitivity label

1.8.2.1.3. Microsoft Teams admin center

A Microsoft Teams Administrator can change or select a sensitivity label at the Microsoft Teams admin center. After choosing a team and moving to the settings, the label can be set or change for the Team.

1. Navigate to the **Microsoft 365 admin center** at https://admin.microsoft.com/
2. Select **… Show all** and **Teams**.
3. In the **Microsoft Teams admin center**, navigate to **Teams** > **Manage teams.**
4. Select the checkmark left of an existing team that you want to apply the published Sensitivity Label to.
5. Select **Edit**
6. Select **Sensitivity** and chose the desired label for the team.



1.8.2.1.4. Microsoft Teams creation controls for sensitivity labeling

If sensitivity labels are created with a Group & site setting and the user has an Azure AD P1 license, then it´s possible to control the creation of Microsoft Teams with sensitivity Labeling.

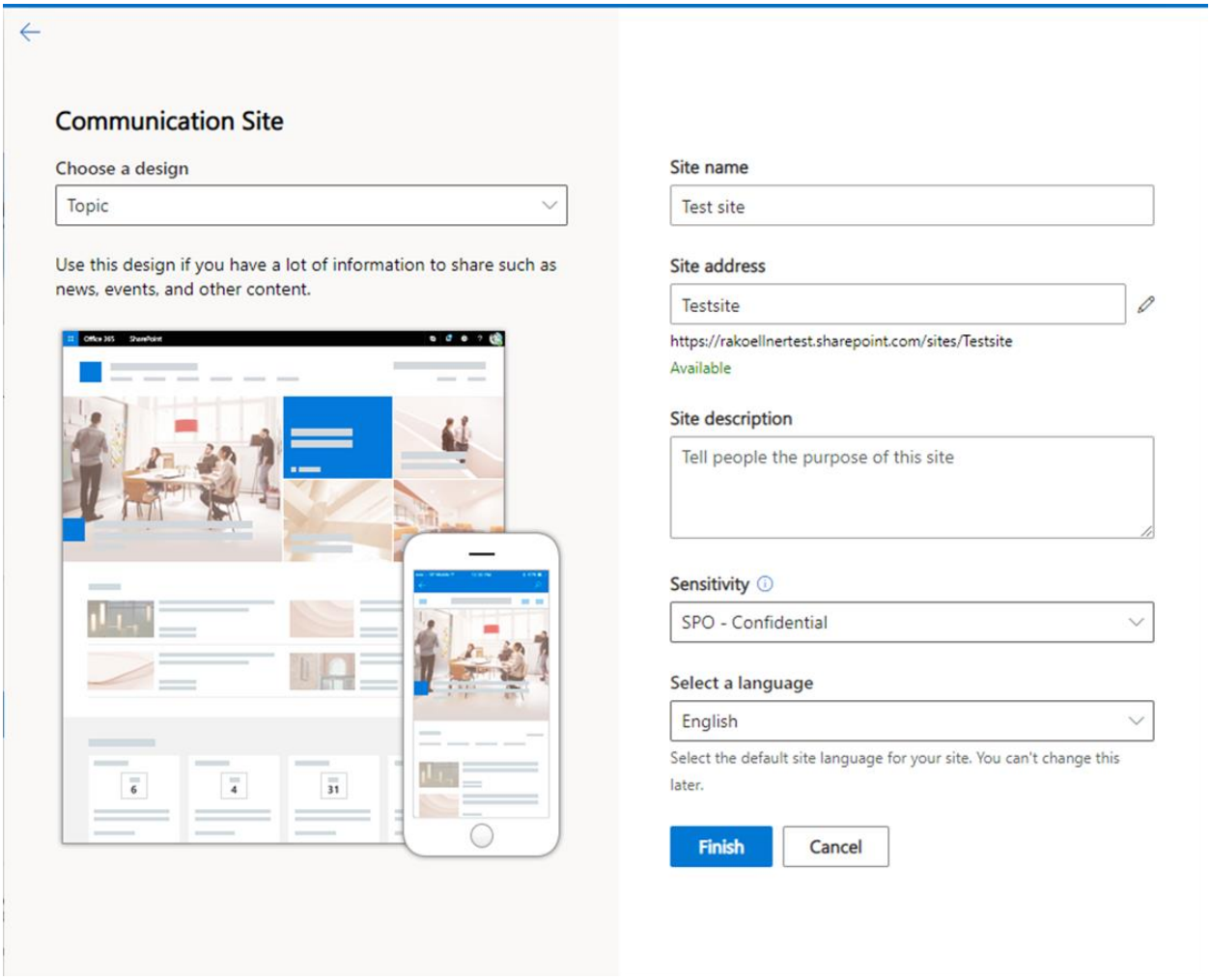
1. Open the Teams desktop client.
2. From the bottom left menu, select **Join or create a team.**
3. Select **Create team.**
4. Select a team template.
5. Select a **published sensitivity label.**
6. Select the **privacy** option. The privacy options available are set within the sensitivity label.
7. Enter a meaningful **Team name** and **description.**
8. Optionally select the team members who should have security access to the team.
9. Select **Close.**

The sensitivity label applies to the Microsoft Team, SharePoint Site and to the private channel SharePoint Site.

1.8.2.1.5. New SharePoint site wizard (user)

In the default wizard, it´s possible to select a sensitivity label. This option is only displayed when the feature is enabled. Under the topic "Sensitivity" the user can select the labels, which are available for them.

1. Navigate to the **Microsoft 365 admin center** at https://admin.microsoft.com/.
2. Select **… Show all** and **SharePoint**.
3. Navigate to **Sites** > **Active** sites.
4. Select + **Create.**
5. Select an appropriate **Design.**
6. Enter a meaningful **Site name**, **Group owner** for the required fields and enter the optional fields as required.

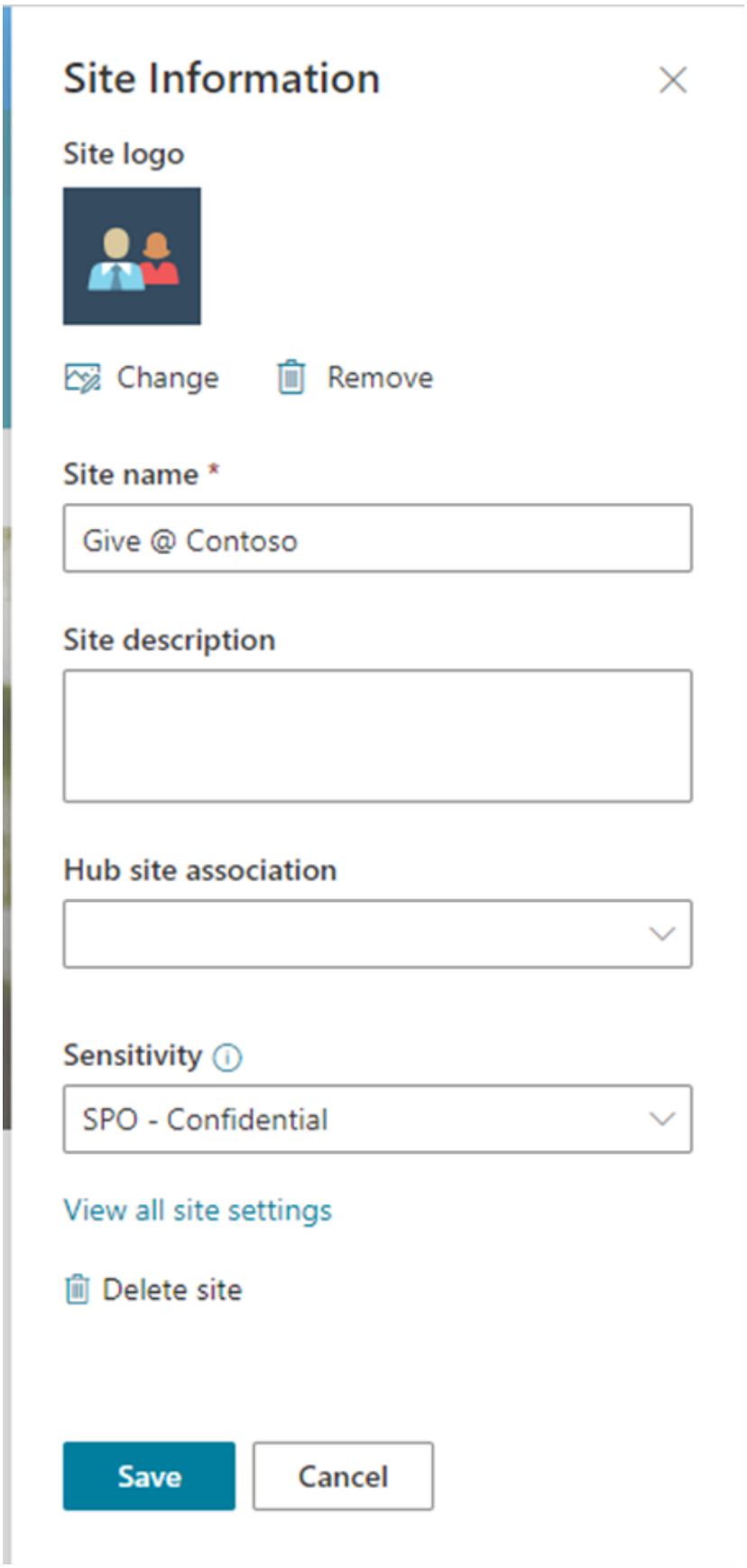


7. Select the Published sensitivity label.
8. Select Finish to create the SharePoint site.

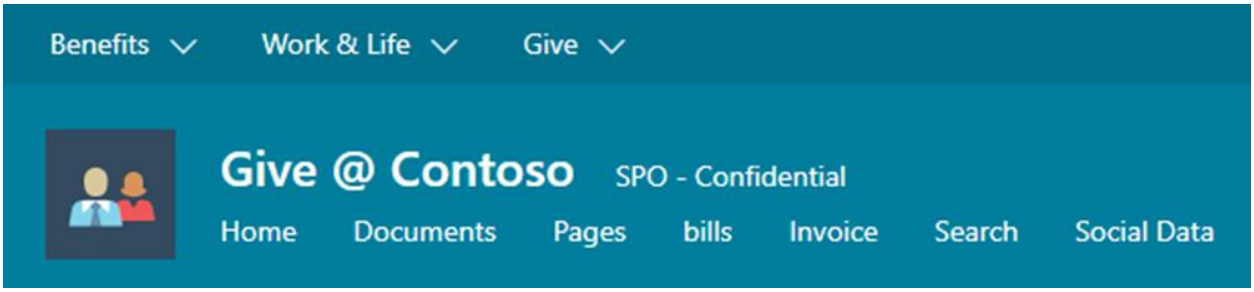
1.8.2.1.6. Applying a label to an existing SharePoint site (user)

If the SharePoint Site is deployed, the label can be changed to handle a lifecycle of the site. The label option is displayed under site information for site administrators.

1. Navigate to an existing **SharePoint online site**.
2. In the top right corner, select the **setting icon (Gear/Cog icon).**
3. Navigate to **Site Information.**
4. Set the **Sensitivity label.**
5. Select **Save.**


Site Information
Site logo
Change
Remove
Site name *
Give @ Contoso
Site description
Hub site association
Sensitivity
SPO - Confidential
View all site settings
Delete site
Save
Cancel

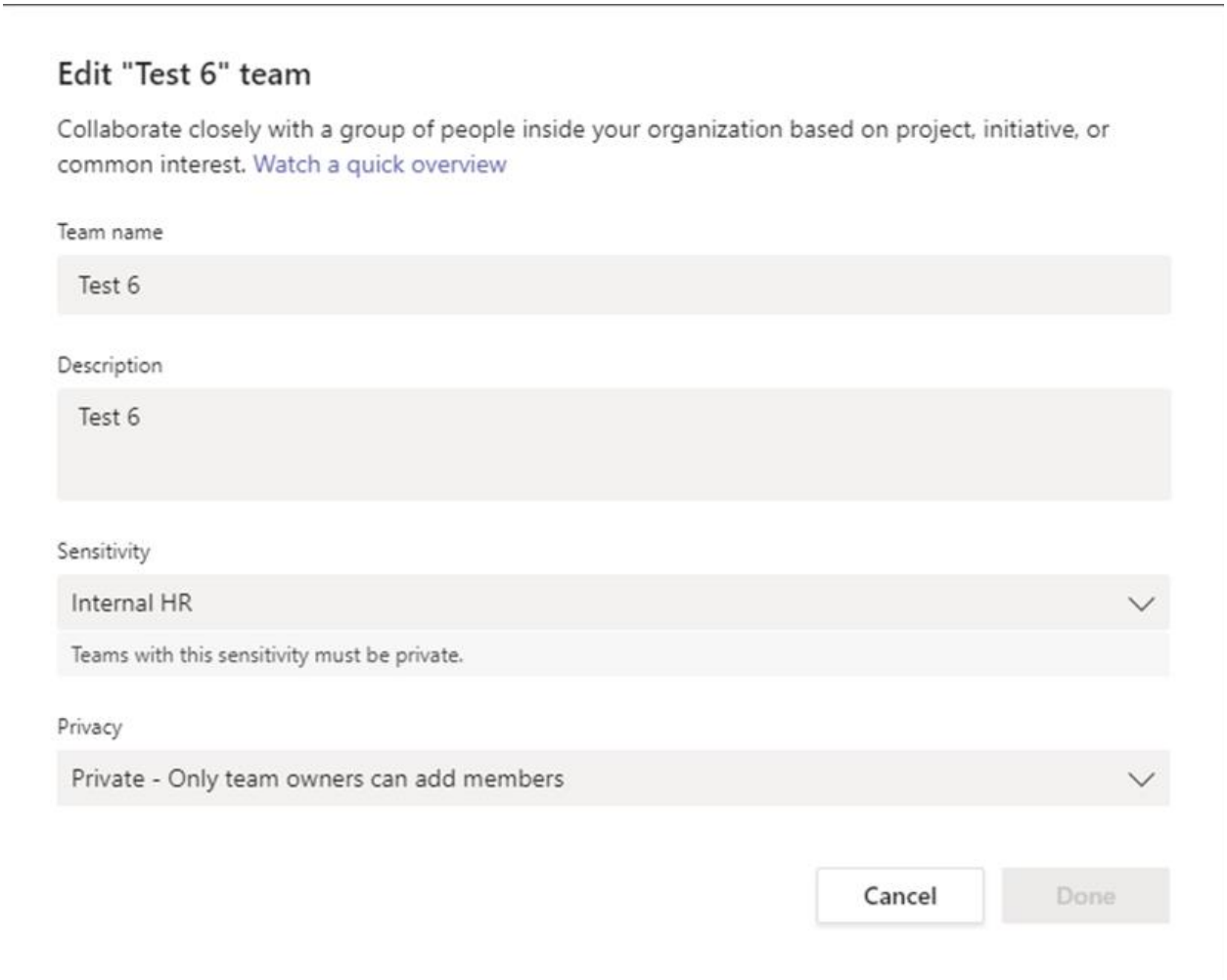
The label will be displayed near to the site name after some time.



1.8.2.1.7. Applying and changing a label to a Microsoft Teams team as a user with a life-cycle example

As a Microsoft Team's Owner you can change the label of a Microsoft Team to handle the lifecycle.

1. Within the Teams application.
2. Navigate to **Teams**
3. Within the **Your teams** list select the required team
4. For the selected team, select **[…]** > **Edit team**
5. Set the **Sensitivity Label.**
6. Select **done.**



1.8.3. Plan on-premises labeling

Adding on-premises files to an information protection solution is important in a hybrid scenario and when migrating into the cloud configurations.

1.8.3.1. Requirements for on-premises labeling

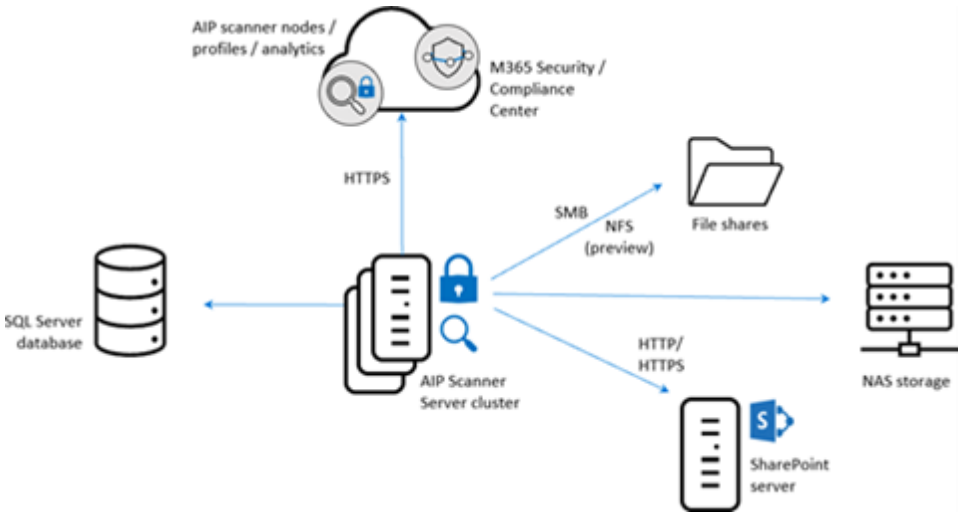
The Unified Labeling Scanner enables you to label on-premises files. Here are some examples of when you might require the scanner:

- Legal requirements from the legal department and purchasing department
- Store only on-premises (example: contract between companies)
- Label and Protect at first
- Data privacy requirements from the data protection officer like:
- To label files before uploading them into the Cloud
- Handling sensitive data in a special way

- Storing files from the data privacy team or the working council on-premises only
- Requirements of an Information Protection Protect Officer
- Know your on-premises data with a scan
- Requirements of the Industry sector
- Storing data only in specific territory
- Storing data only in a specific information protection system

1.8.3.2. Requirements and best practices for the unified labeling scanner

The Azure Information Protection unified labeling scanner scans and protects files in on-premises environments like NAS storages, file shares, and local SharePoint servers.



The table below lists locations where it's possible to scan with the Unified Labeling Scanner:

Product	Version
SharePoint libraries and folder	SharePoint Server 2019 through SharePoint Server 2013 and SharePoint Server 2010 for customers with extended support.
UNC Path	Network shares that use the SMB or NFS (Preview) protocols

To classify and protect your files, the scanner uses sensitivity labels configured in any of the following Microsoft 365 labeling admin center including:

- Microsoft 365 Security Center
- Microsoft 365 Compliance Center

1.8.3.2.1. Requirements for the unified labeling scanner

The following requirements must be fulfilled before installing the Unified Labeling Scanner:

- SQL Server database installed (SQL Express for Example)
- The SQL server database stores the labeling information and all information about the scanning process and the files, which are scanned.
- The Unified Labeling Client executable including the Scanner.
- One of the following roles: Compliance administrator or Compliance data administrator or Security administrator permissions or Global administrator.
- A configured Azure AD token.
- Any Windows Server 2016 to Windows Server 2019 with UI.

1.8.3.2.2. Service accounts needed

For the installation and to run the scanner the following service accounts are needed:

Requirement	Details
Log on locally user right assignment	Required to install and configure the scanner, but not required to run scans. Once you've confirmed that the scanner can discover, classify, and protect files, you can remove this right from the service account.
Log on as a service user right assignment.	This right is automatically granted to the service account during the scanner installation and this right is required for the installation, configuration, and operation of the scanner.
Permissions to the data repositories	*File shares or local files*: Grant Read, Write, and Modify permissions for scanning the files and then applying classification and protection as configured.SharePoint: You must grant Full Control permissions for scanning the files and then applying classification and protection to the files that meet the conditions in the Azure Information Protection policy. *Discovery mode*: To run the scanner in discovery mode only, Read permission is sufficient.
For labels that reprotect or remove protection	To ensure that the scanner always has access to protected files, make this account a super user for Azure Information Protection, and ensure that the super user feature is enabled. Additionally, if you've implemented onboarding controls for a phased deployment, make sure that the service account is included in the onboarding controls you've configured.

Requirement	Details
Specific URL level scanning:	To scan and discover sites and subsites under a specific URL, grant Site Collector Auditor rights to the scanner account on the farm level.

1.8.4. Configure on-premises labeling for the Unified Labeling Scanner

The installation and configuration of the Unified Labeling Scanner is done from the AIPService PowerShell module on a server that will act as the Unified Labeling Scanner in an environment.

1.8.4.1.1. Installation of the unified labeling scanner

After fulfilling the requirements like service accounts and a SQL Server instance, it´s possible to install the Unified Labeling Scanner in the following steps:

1. Install and sign into a Windows Server computer or VM.
2. Install the Unified Labeling Client on the machine.
3. Run the Windows PowerShell as local administrator in an elevated command shell.
4. Run the cmdlet from the AIPService PowerShell module to install the AIP Scanner:

   ```
   Install-AIPScanner -SqlServerInstance <name> -Cluster <cluster name>
   ```

5. Verify that the service is now installed by using Administrative Tools > Services. The installed service is named Azure Information Protection Scanner and is configured to run by using the scanner service account that you created.
6. You can control the installation and operation in the Task Manager of the Windows Server, which is the host for the scanner.

1.8.4.1.2. Configuration of the unified labeling scanner

The Unified label is installed on a Windows server and is connected to the SQL Server instance. In the next steps to configure the Scanner we need to connect the local instance with the Azure environment with an Azure AD Token and after it we can configure it to make the first run.

1.8.4.1.3. Acquire an Azure AD Token for the scanner

Perform the following steps to fetch an Azure AD Token for the Unified Labeling Scanner:

1. Navigate to the **Azure portal** at https://portal.azure.com.
2. In the top search bar, enter **App Registrations** and select **App registrations**.
3. Select + **New registration**.
4. Provide a meaningful **name**.
5. Select the **Supported account type** (or leave as default).
6. Set the **Redirect url** to: https://localhost
7. Select **Register.**
8. The overview page provides the **Application (client) ID**, copy this ID for use later.
9. Select the **Certificates & secrets** setting.
10. Under **Client secrets**, select + **New client secret** to create a new secret.
11. Provide a **description** for the secret and choose the desired **expiration interval**.
12. Immediately copy the value of the **new secret** to a secure location. The full value is displayed to you only once.
13. Select **Add.**
14. Navigate to **API Permissions.**
15. Select + **Add a permission.**
16. Select **Azure Rights Management Services** > **application permissions.**
17. Expand the **content** permissions.
18. Select **Content.DelegatedReader** and **Content.DelegatedWriter.**
19. Select **Add Permission.**
20. Select + **Add a permission** > **APIs my organization uses.**
21. Search for **Microsoft Information Protection Sync Service.**
22. Select **Microsoft Information Protection Sync Service** > **Application permissions.**
23. Expand the **content** permissions.
24. Select **UnifiedPolicy.Tenant.Read**.
25. Select **Add Permission**.
26. Select the **Grant admin consent button.**
27. Navigate to the **Azure Active Directory.**
28. Within the overview page copy, the **Tenant ID** required for the next step.
29. Configure the Azure AD applications for **Set-AIP Authentications** from the Windows Server computer, if your scanner service account has been granted the Log-on locally right for the installation, sign in with this account and start a PowerShell session using the **AzureInformationProtection** module.

```
Set-AIPAuthentication -AppId <ID of the registered app> -AppSecret <client secret
sting> -TenantId <your tenant ID> -DelegatedUser <Azure AD account>
```

30. After this cmdlet is run the scanner will have an Azure AD Token and be registered as an application in the Azure environment. With this connection, the scanner has access to the label scheme and the settings.

1.8.4.1.4. Configuration of the scanner and scan methods

The configuration for the scanner is done in the Azure portal. Follow these steps to configure and set up the Scanner to perform scans in an organization's network:

1. Sign into the **Azure portal** at https://portal.azure.com.
2. The user requires one of the roles (requirements).
3. Create a scanner cluster.
4. Scan your network for risky repositions (optional).
5. Run your network scan job (Public Preview).
6. Create a content scan job.
7. Start the Scan.

Moreover, it´s also possible to restart the scan and rescan all the files.

The Unified Labeling scanner does not scan and protect in real time. The crawler runs a cycle and repeat.

1.8.4.2. Operational scenarios for the unified labeling scanner

The Unified labeling scanner can be used for different operational scenarios, some of them include:

Scenario	Scanner run
Scan for a report only to know your data	Run the scanner in discovery mode only to create reports that check to see what happens when your files are labeled.
Run the scanner to find and discover files with sensitive information	Run the scanner to discover files with sensitive information, without configuring labels that apply automatic classification.
Run and apply labels	Run the scanner automatically to apply labels as configured.
Specific scan only a few files types	Define a file types list to specify specific files to scan or to exclude.

1.8.5. Apply protections and restrictions to email and files

Users can apply just one label at a time for each document or email. When you label an email message that has attachments, the attachments don't inherit the label with one exception:

- The attachment is an Office document with a label that doesn't apply encryption, and the label you apply to the email message applies encryption. In this case, the emailed Office document inherits the email's label with its encryption settings.

Otherwise:

- If the attachments have a label, they keep their originally applied label.
- If the attachments are encrypted without a label, the encryption remains but they aren't labeled.
- If the attachments don't have a label, they remain unlabeled.

1.8.5.1. Applying labels to emails manually

You can apply a sensitivity label manually in the Outlook Desktop app (Mac, Windows), on the mobile Outlook app (iOS, Android) or in the WebApp.

1.8.5.2. Applying by default with auto apply

It´s possible to apply a sensitivity label by default using auto-apply functionality.

Options to auto apply a label to a file and email:

- Default label for new emails and documents
- Auto apply by sensitive information types / with or without a hint
- Auto apply by trainable classifiers

1.8.5.3. Restrictions with a sensitivity label template using auto-apply

There are sensitivity label templates. These templates have their own restrictions and are typically protection templates like the default ones (encrypt only and do not forward), which can be selected by the user. In this case, there are restrictions coming with the email and one with the file that's part of the email. The email is only the container of the files that may have their own protection configuration.

1.8.5.4. Applying protections to files

When a file is protected with a sensitivity label, the protection is sensitive at the file level. Even if the file's storage location changes or is shared via email or other sharing tools; the file remains protected.

Encryption of a file and access restrictions are connected. Without encryption it´s not possible to restrict access.

1.8.6. Monitor label performance using label analytics

Applying a label to a file, an email, a SharePoint Site, or a Microsoft Team is a great option to control access and sharing options.

1.8.6.1. Pulling a report

The sensitivity labels are a part of the Reporting system in the Security and the Compliance center. For sensitivity labeling, we will focus on the Microsoft 365 compliance center reports.

An existing sensitivity label report may be accessed with these steps:

1. Navigate to the **Microsoft 365 compliance center** at https://compliance.microsoft.com.
2. Navigate to **Reports**.
3. Within the Labels area, select **View details** for one of the boxes that provide reporting data of interest.

The Organizational data of this dashboard provides an overview of the DLP matches that occurred in SharePoint, OneDrive, Exchange Online, or Microsoft Teams.

Tip

The reports in the Reports area are based on the organizational level information. For reports in detail and on a user level, please choose Microsoft Defender for Apps or the Data classification area with the Content explorer and the Activity explorer.

1.8.6.2. Planning log analytics

Log analytics is a tool in Azure portal. A log analytics workspace is required to use Azure Information Protection to gather information for these organizational reports. To start log analytics, you must create a Log Analytics workspace to collect and analyze the

information. You need an additional Azure Subscription to create a Log Analytics workspace.

1.8.6.3. Roles required for log analytics

To create your Log Analytics workspace or to create custom queries, you need one of the following roles:

- Azure Information Protection administrator
- Security administrator
- Compliance administrator
- Compliance data administrator
- Global administrator

After the workspace has been created, you can then use the following roles with lower permissions to view the data collected:

- Security reader
- Global reader

To create the workspace or to create custom queries, you need one of the following:

- Log Analytics Contributor
- Contributor
- Owner

After the workspace has been created, you can then use one of the following roles with lower permissions to view the data collected:

- Log Analytics Reader
- Reader

1.8.6.3.1. Understanding the storage requirements

The amount of data collected and stored in your Azure Information Protection workspace will vary significantly for each tenant, depending on factors such as how many Azure Information Protection clients and other supported endpoints you have, whether you're collecting endpoint discovery data, you've deployed scanners, the number of protected documents that are accessed, and so on.

1.8.6.4. Monitoring with Microsoft Sentinel

A Sensitivity Label monitoring and analyzing is also possible with Microsoft Sentinel workspace. The Log files will be collected by Microsoft Sentinel to get an overview of the entire environment with all signals.

1.8.7. Knowledge check

1.8.7.1. Question

1. If you want to restrict access to a file, you need to configure a sensitivity label with which of the following?

- Marking content
- Encryption
- Guest access

1.8.7.1.1. Correct Answer

- Encryption

This answer is correct. Only a label with encryption can have a access rules to prevent other user to edit or open the file.

1.8.7.1.2. Wrong Answer

- Marking content

The answer is incorrect. Only marking a content is not the way to restrict access to a file.

- Guest access

The answer is incorrect. The Guest access prevention is only an option, but with it it´s not possible to restrict file access in detail.

1.8.7.2. Question

2. The Unified Labeling Scanner requires which other system to conduct scans?

- a SQL Server Standard or SQL Server Enterprise
- Microsoft 365 alerts enabled.

- A Linux server.

1.8.7.2.1. Correct Answer

- a SQL Server Standard or SQL Server Enterprise

This answer is correct. The SQL Server Express version is only for testing.

1.8.7.2.2. Wrong Answer

- Microsoft 365 alerts enabled.

The answer is incorrect.

- A Linux server.

The answer is incorrect. A Windows server is needed.

2. Implement Data Loss Prevention

2.1.Prevent data loss in Microsoft 365

2.1.1. Introduction

Microsoft 365 compliance includes data loss prevention capabilities to help you prevent accidental and intentional data loss for your sensitive information. Sensitive information can include financial data or personal information such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically protect sensitive information across Microsoft 365.

Suppose you're the administrator for your organization, responsible for information protection, including preventing inadvertent data loss. This module will walk you through the concepts, procedures, and best practices to configure data loss prevention policies in your organization.

2.1.2. Data loss prevention overview

To comply with business standards and industry regulations, it's critical that your organization protects sensitive information to prevent its inadvertent disclosure. Sensitive information can include financial data, health records, credit card numbers, social security numbers, and employee evaluations. Use data loss prevention (DLP) policies to identify, monitor, and automatically protect sensitive information across Microsoft 365. Microsoft DLP helps prevent users from accidentally, rather than

intentionally sharing sensitive content. (If a user is determined enough to send sensitive data outside the organization, they will find another way to do so.)

2.1.2.1. DLP policies can

1. Identify sensitive information across many locations including:
   1.1. Exchange Online
   1.2. SharePoint Online
   1.3. OneDrive for Business
   1.4. Microsoft Teams
   1.5. Windows devices
2. Monitor and protect sensitive information in Excel, PowerPoint, Word, and Outlook.
3. Prevent the accidental sharing of sensitive information.
4. Educate users on staying compliant without interrupting their workflow.
5. Produce DLP alerts and reports showing content that matches your organization's DLP policies.

2.1.2.2. Each DLP policy contains

2.1.2.2.1. Where to protect the content

Content is protected in locations like SharePoint Online, Exchange Online, OneDrive for Business accounts, Microsoft Teams chat and channel messages, and Windows 10 devices.

2.1.2.2.2. When and how to protect the content

When and how to protect the content is defined by enforcing rules. A policy contains one or more rules, and each rule consists of conditions and actions at a minimum. For each rule, when the conditions are met, the actions are taken automatically.

2.1.2.2.2.1. Conditions

Circumstances under which a rule is enforced. For example, a condition might be configured to look only for content containing credit card information that has been shared with people outside the organization, but they can be must more sophisticated, as well.

2.1.2.2.2.2. Actions

Define what happens when content matching the conditions is identified. An action could be to block access to a document and send the user and compliance manager an

email notification. The complexity of the actions you specify are based on your business requirements.

You don't want a new DLP policy to unintentionally block access to thousands of documents users require access to. DLP policies should be rolled out gradually to assess their impact and test their effectiveness. Here is a three-step process to implementing DLP policies to minimize the risk of unintended consequences:

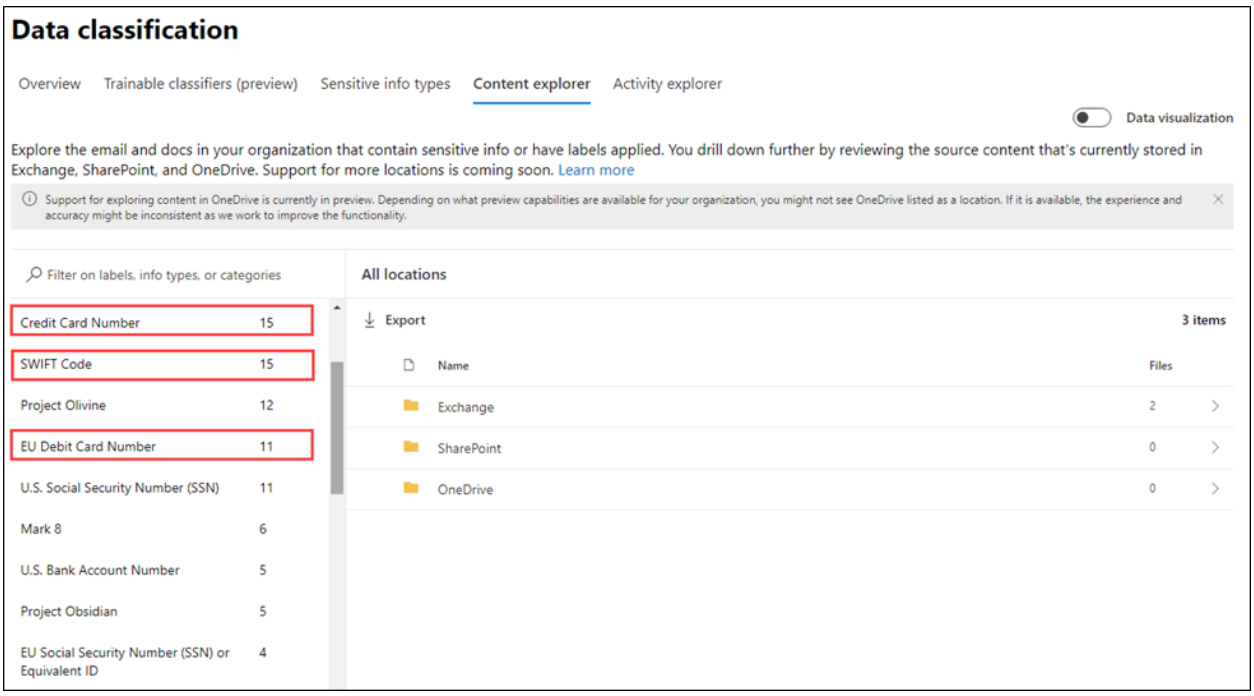
1. Start in test mode without policy tips. Use the DLP reports and incident reports to assess the impact of the policy. You can use DLP reports to view the number, location, type, and severity of policy matches. Based on the results, you can fine-tune the rules as needed. Configuring a DLP policy in this way will not impact user productivity.
2. Move to test mode with notifications and policy tips. Adding notifications and policy tips gives you the opportunity to educate users about your compliance policies and prepare them for the rules that are going to be applied. At this stage, you can also ask users to report false positives so that you can refine the rules.
3. Start full enforcement. The actions in the rules are applied and the content is protected once full enforcement is in place. Continue to monitor the DLP reports and any incident reports or notifications to make sure that the results are what you intend.

2.1.3. Identify content to protect

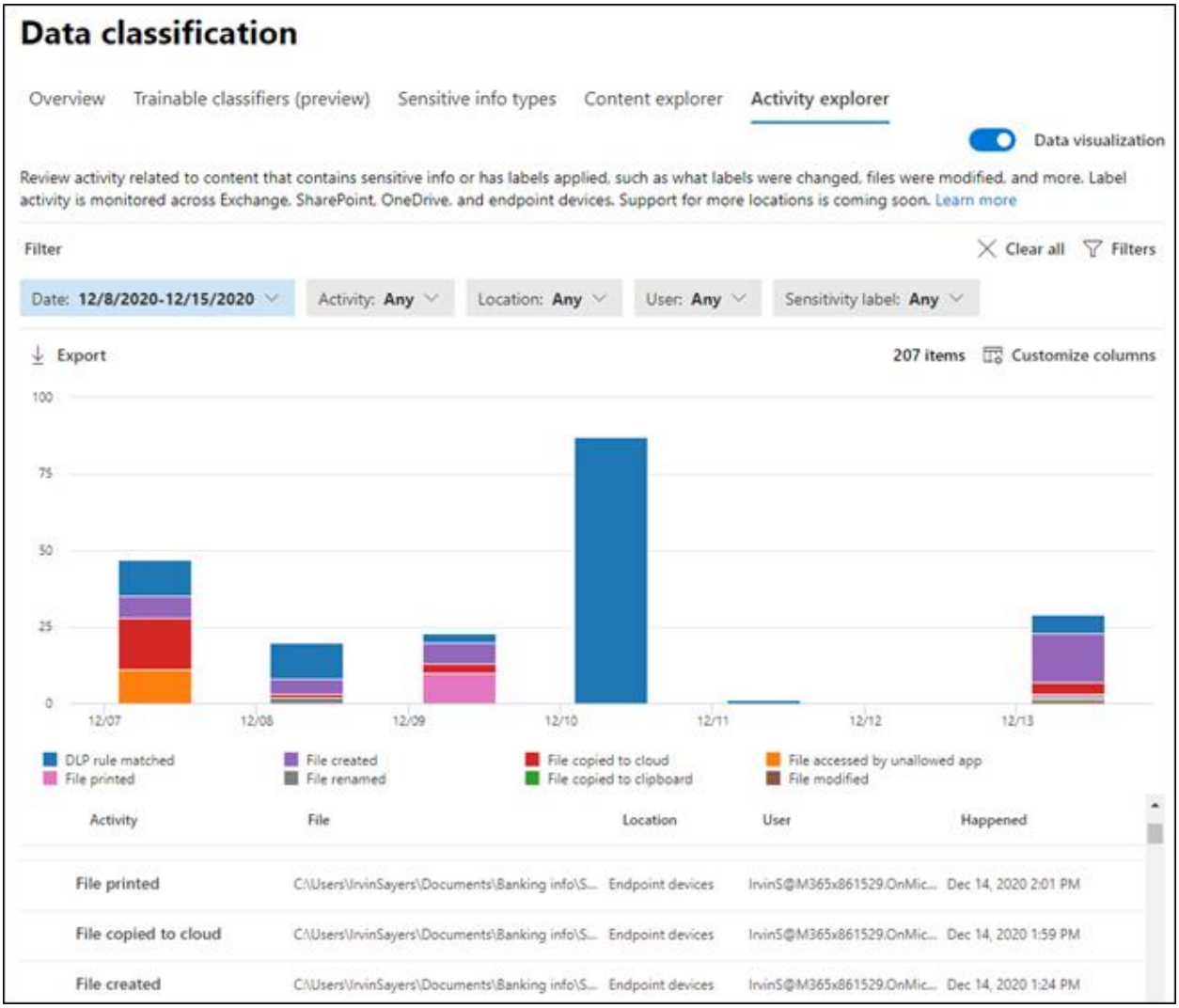
The Microsoft 365 data classification solution is a great place to start understanding what sensitive information might need to be protected.

Content explorer identifies the email and documents in your organization that contain sensitive information. The image below shows a list of all the sensitive information content explorer identified in SharePoint, OneDrive, and Exchange. Content explorer uses the built-in sensitive info types included in Microsoft 365 compliance and any custom sensitive info types you define to identify the content. If only using built-in sensitive info types, no configuration is needed to allow you to understand the data you might want to protect.

The highlighted items are the three sensitive information types that informed the creation of the U.K. Financial Data DLP policy we will be using in our examples.



Activity explorer, shown in the image below, includes information on activity related to content that contains sensitive information, which can also inform what should be protected by DLP policies. The top portion of the screen includes a histogram of various activities over time, while the bottom portion lists each recorded activity. Like content explorer, much of the data generated by activity explorer requires little or no configuration.



2.1.4. Define policy settings for your DLP policy

There are two different workflows when you define policy settings: simple and advanced. The simple workflow starts if you choose the **Review and customize default settings from the template** option on the **Define policy settings** page. The more advanced flow is initiated if you choose **Create or customize advanced DLP rules**.

2.1.4.1. Simple workflow

The simple workflow lets you quickly:

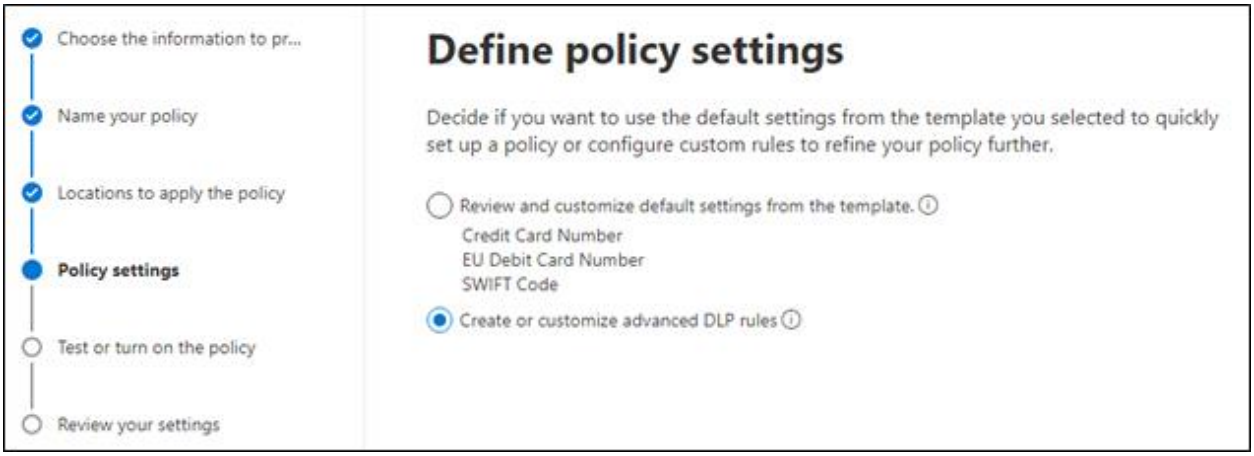
1. Specify the sensitive info types or labels you want to protect.
2. Decide whether you want the policy to detect when the content is shared inside or outside your organization.
3. Set up actions like access restrictions and user and admin notifications.

Select this option if you want to quickly set up a policy that protects content based only on the sensitive information types from the policy template selected earlier.

2.1.4.2. Advanced workflow

The advanced workflow uses a rule editor to extend the options offered in the simple flow. You can use the advanced flow to refine the policy using rules that include more conditions, exceptions, and actions. The advanced workflow branch is also the only option available if Custom is selected during the Choose locations to apply the policy step.

The image below shows the two workflow branches. Notice in the simple branch, listed first, the three sensitive information types that were inherited from the selection of the **U.K. Financial Data** policy template in the **Choose information to protect** step. We're going to use the advanced option in our examples, so the image shows Create or customize advanced DLP rules has been selected.

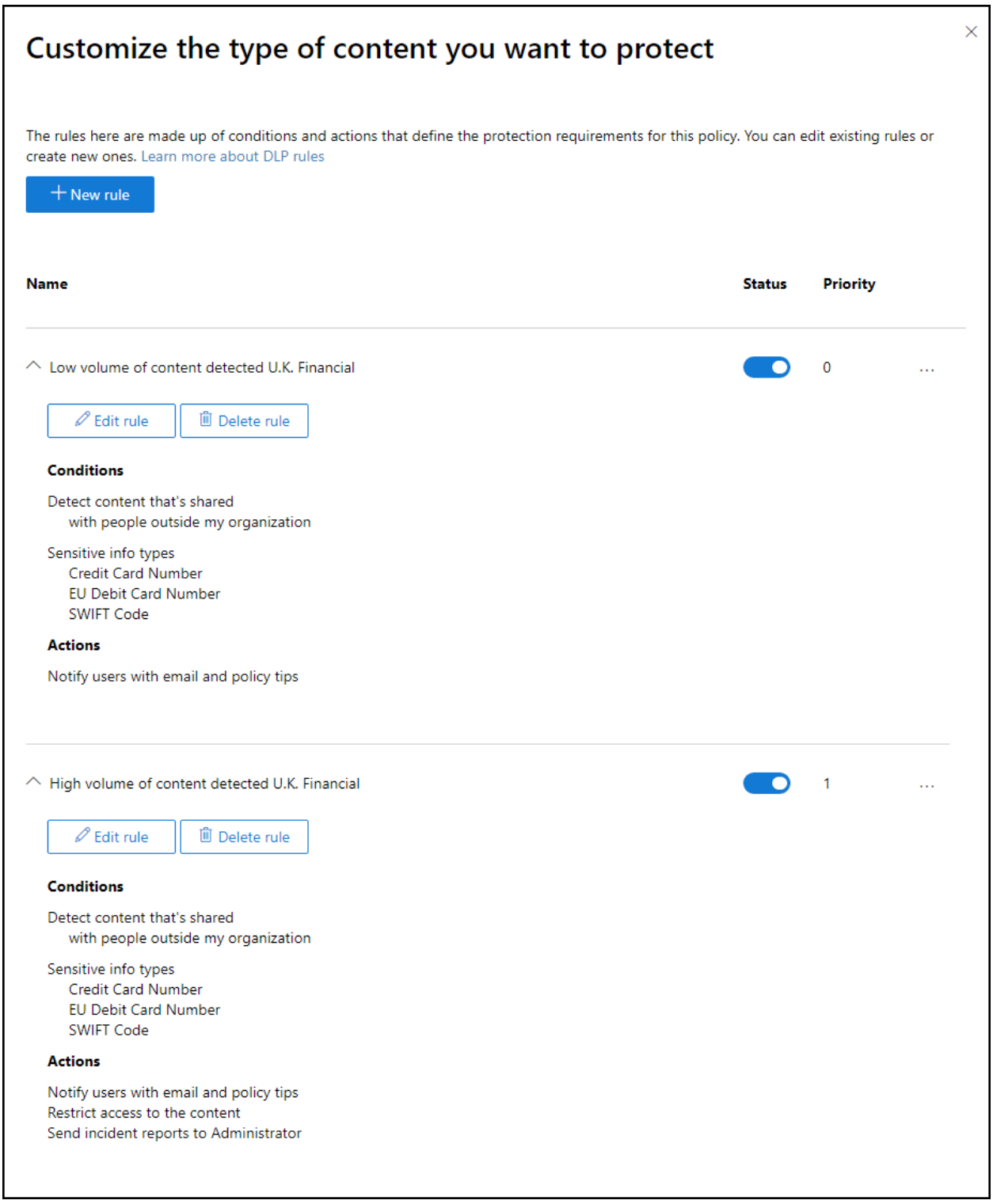


2.1.4.3. Customize advanced DLP rules

Two rules are defined by default when you use a policy template and follow the advanced DLP rules workflow branch. If you choose the **Custom** option, you have to define your own rules. You can also edit any existing rules, delete them, or create new ones. The only requirement is you must define at least one rule before you can move to the next step in the process.

Using the **U.K. Financial Data** policy template we started with earlier, the image below shows a summary of the two default rules associated with this DLP policy. One rule is for detecting a low volume of content, and a second rule is for detecting a high volume of content. Notice in the image below the Actions listed in the two rules are different. One

set of actions is defined for when a low volume of content is detected, and a different set of actions is defined for when a high volume of data is detected. This allows you to respond differently based on the seriousness of the policy violation. For example, sending an email that includes one to two credit card numbers might be deemed acceptable and addressed with a simple warning to the user, while sending one with 1,000 credit card numbers may be considered a critical security breach and call for a different response entirely. It is up to your organization to decide how to respond and configure the DLP policy rules accordingly.


Customize the type of content you want to protect
The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones. Learn more about DLP rules
New rule
Name
Status
Priority
Low volume of content detected U.K. Financial
0
Edit rule
Delete rule
Conditions
Detect content that's shared with people outside my organization
Sensitive info types
Credit Card Number
EU Debit Card Number
SWIFT Code
Actions
Notify users with email and policy tips
High volume of content detected U.K. Financial
1
Edit rule
Delete rule
Conditions
Detect content that's shared with people outside my organization
Sensitive info types
Credit Card Number
EU Debit Card Number
SWIFT Code
Actions
Notify users with email and policy tips
Restrict access to the content
Send incident reports to Administrator

2.1.4.4. Review the U.K. Financial Data policy settings

You edit all of the rules included with the DLP policy template - you can edit *all* of the DLP policy rules. Even the default rules should be reviewed to determine they meet your requirements. Rules can include:

2.1.4.4.1. Conditions

Determine what types of information you are looking for, and when to take an action.

2.1.4.4.2. Exceptions

Prevents the application of a rule for content matching the exceptions.

2.1.4.4.3. Actions

When content matches a condition in a rule, you can apply actions to automatically protect the content.

2.1.4.4.4. User notifications

Use notifications to educate your users about DLP policies and help them remain compliant without blocking their work.

2.1.4.4.5. User overrides

Allows the user to override the policy and share the content.

2.1.4.4.6. Incident reports

When a rule is matched, you can send an incident report to your compliance officer (or any people you choose) with details of the event.

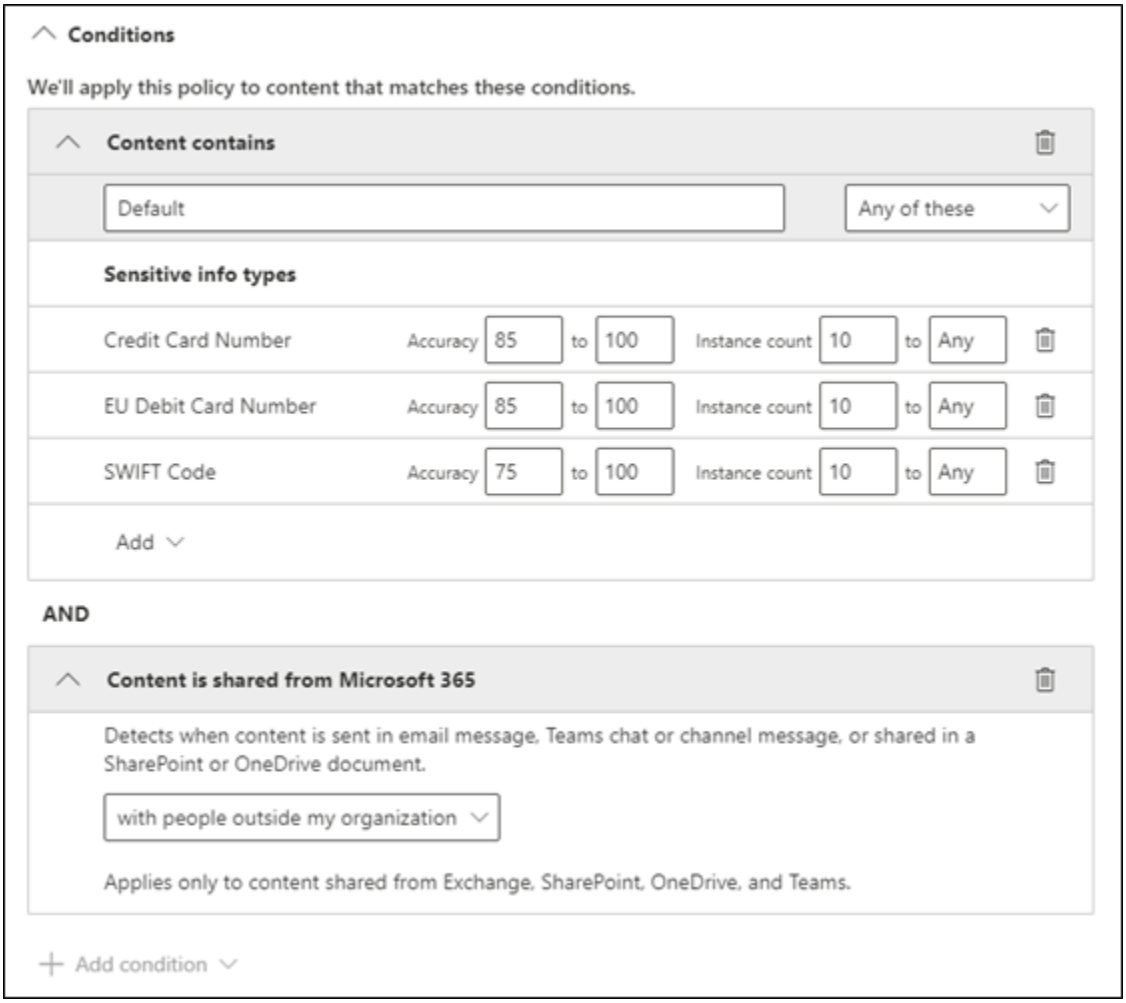
2.1.4.4.7. Options

Provide more options to specify how the DLP policy is processed.

2.1.4.5. Conditions

The image below shows the conditions set in the **High volume of content detected U.K. Financial** rule. Each condition is currently using the default settings from the policy template:

- The *Content contains* condition is relevant to all locations. By default, it looks for any of the three sensitive info types listed that exceed an instance count of 10. You can add extra sensitive info types and modify the lower and upper threshold for the instance count.
- The *Content is shared from Microsoft 365* condition only applies to content shared from Exchange, SharePoint, OneDrive, and Microsoft Teams. It doesn't apply to the Windows 10 devices or Cloud App Security locations. We'll add the Windows 10 devices in the next step.



2.1.4.5.1. Actions

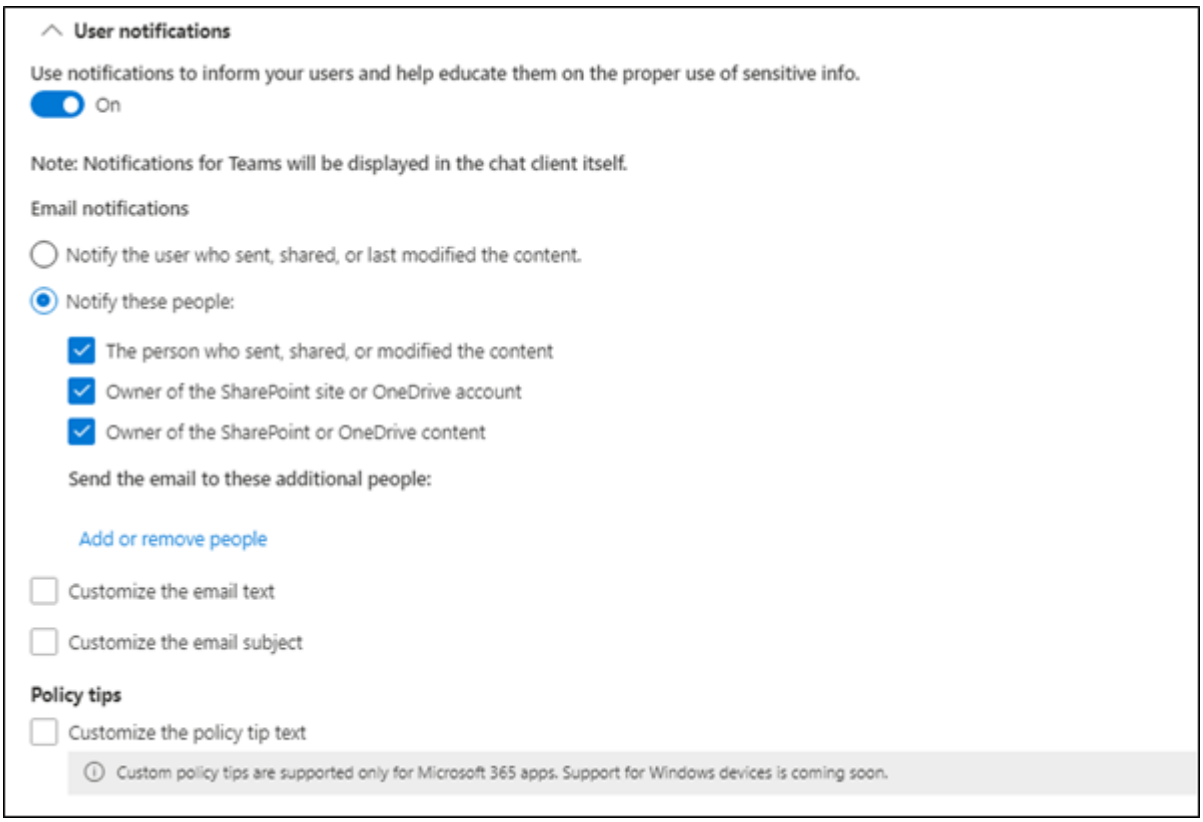
The image below shows the actions in the **High volume of content detected U.K. Financial** rule. By default, users are blocked from sending outside the organization any email or Teams chats and channel messages that contain the type of content you're protecting.

- The *Restrict access or encrypt the content in Microsoft 365 locations* action (enabled by default in this rule) adds files stored in SharePoint, OneDrive, and Teams to the locations where sharing is blocked.
- The *Audit or restrict activities on Windows devices* action isn't included by default. Select it to restrict activities on Windows devices. When the activities listed are detected on Windows devices for supported files containing sensitive info that matches this policy's conditions, you can choose to do any of the following:
    - Audit the activity only
    - Block the activity entirely
    - Block the activity but allow users to override the restriction

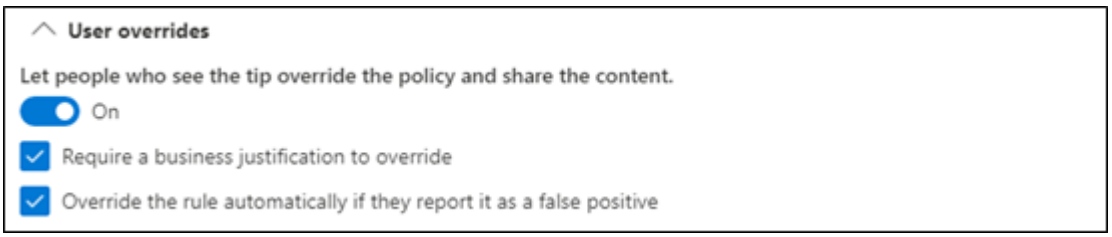
The ability to audit or restrict activities on Windows devices is part of the functionality referred to as "endpoint data loss prevention." In our example, we'll choose to block each type of endpoint activity, like printing and copying sensitive data to the clipboard, but allow users to override it.

2.1.4.5.2. User notifications and overrides

The image below shows the user notifications and overrides in the **High volume of content detected U.K. Financial** rule. User notifications take the form of emails and/or policy tips designed to educate users on the proper use of sensitive information. There may be occasions where you want to notify someone else besides the user and/or customize the message or policy tip that is displayed. You have flexibility in deciding who is informed about the incident and how they are notified.



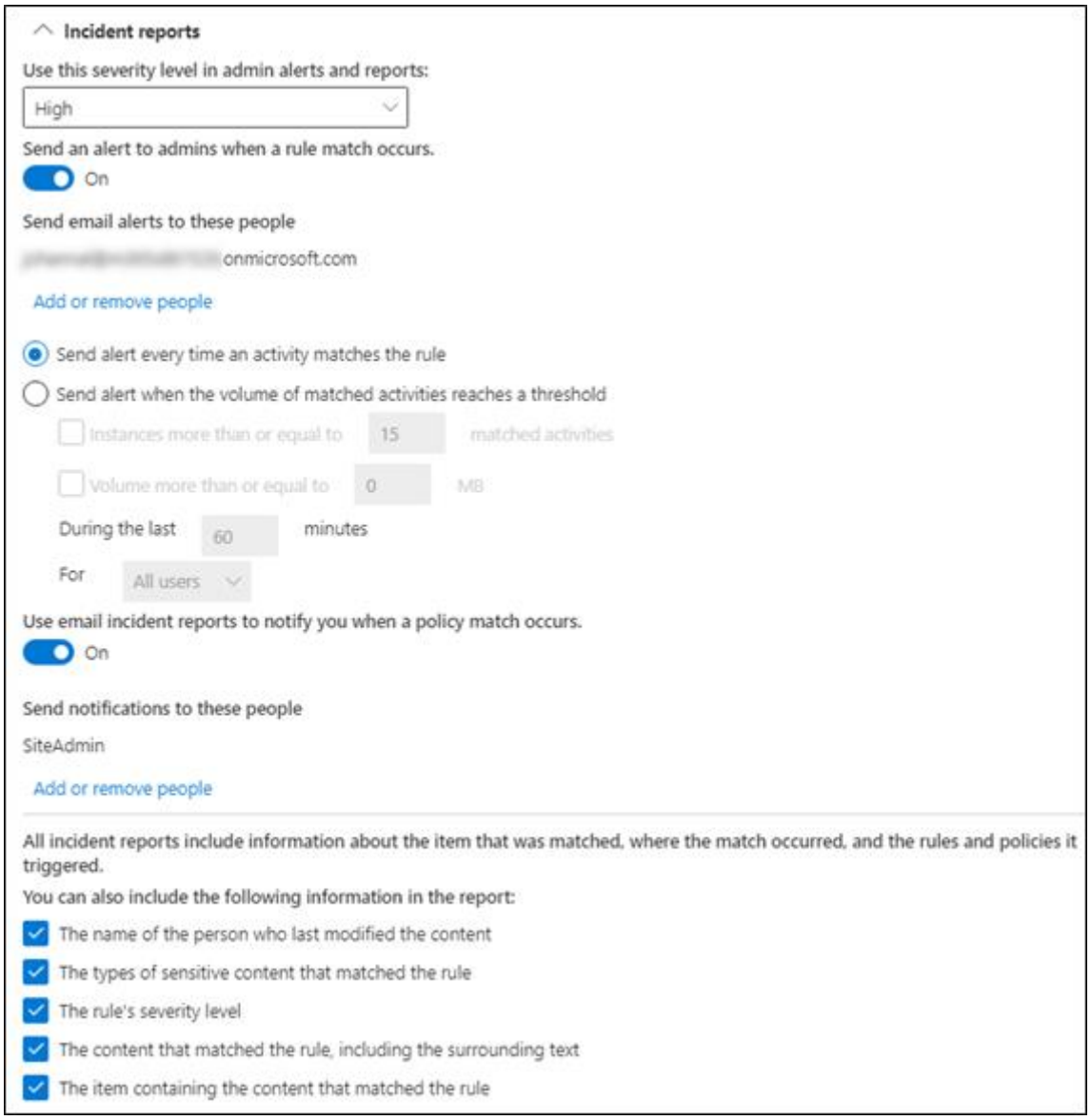
User overrides are disabled by default for the **High volume of content detected U.K. Financial** rule. Enable them as shown in the image below. Options include requiring the user to enter a business justification when overriding the policy and/or allowing the policy to be overridden if the user reports it as false positive. Select both. The settings in this section are not relevant to Windows 10 devices as the override settings for Windows devices are configured under the Actions section in the rule editor.



2.1.4.5.3. Incident reports

When a rule is matched, different types of incident reports can be generated to make those with administrative or oversight responsibilities aware. You can send an incident report to your compliance officer, or anyone you choose, with details of the event. As with user notifications you have several options. In this example, select **Send an alert to admins when a rule match occurs** and **Use email incident reports to notify you**

when a policy match occurs. Set the severity level of **High.** Also select the option to **Send alert when the volume of matched activities reaches a threshold** and then set an instance or volume threshold. (We've used 15 instances in the screenshot below.)



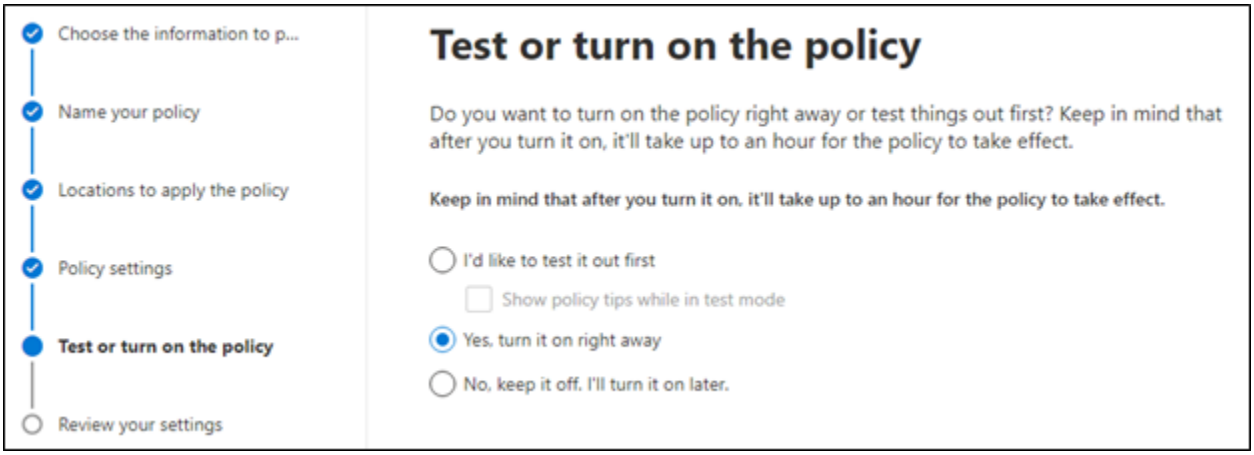
2.1.5. Test and create your DLP policy

Now you're ready to validate your policy settings and then, based on how the policy performs, create the new policy.

2.1.5.1. Test the policy settings

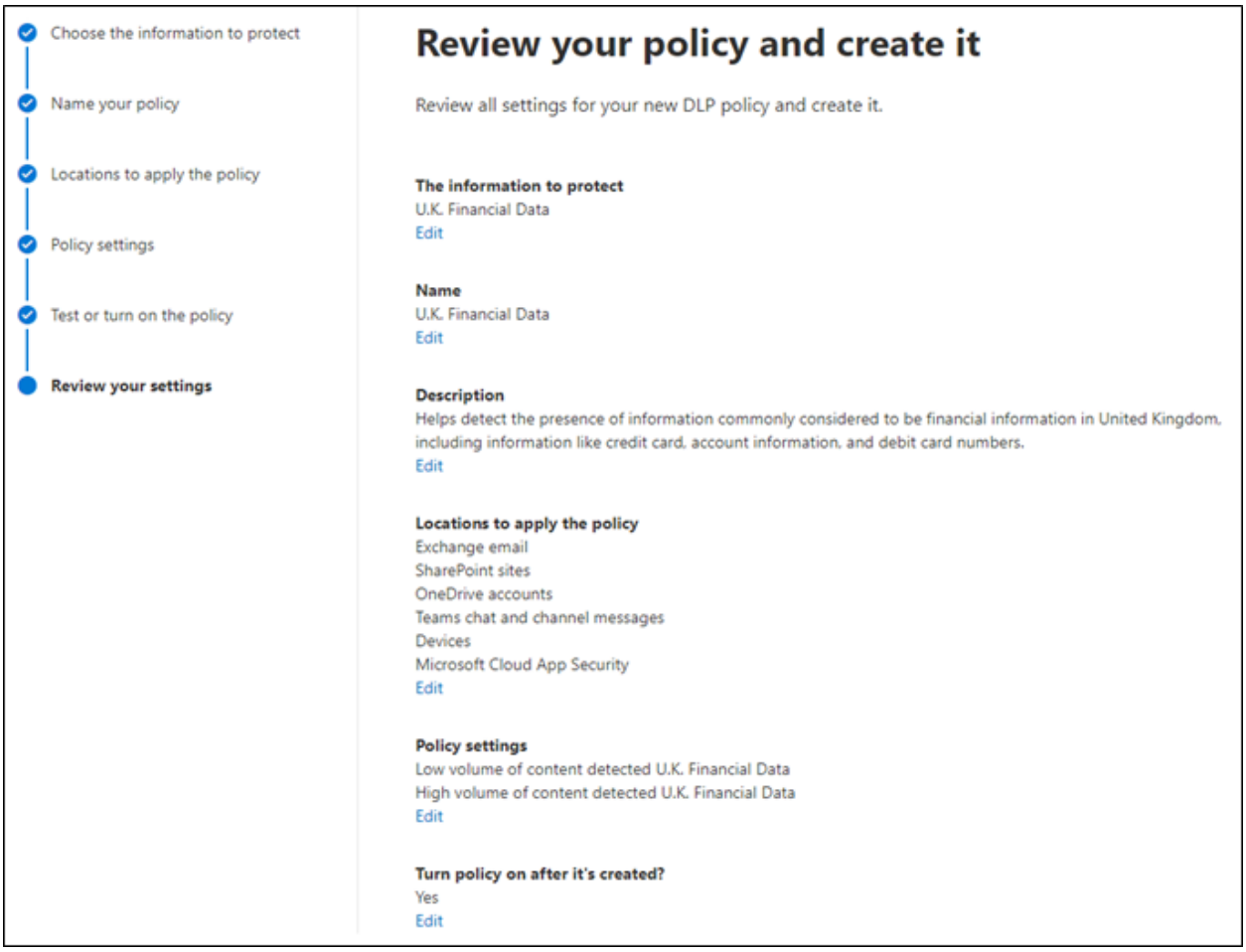
DLP policies can potentially impact every user in the organization. You can use this step to test the policy to evaluate how it will perform prior to enabling it. The first option, *I'd like to test it out first*, is recommended for any new policy you configure or existing policy you modify. You can also elect to show or hide policy tips while testing out the policy to limit the impact on users while you conduct your testing.

The scope for the policy we are creating in our example is all locations. That means it can potentially have a significant impact if configured incorrectly or if an effective user education plan has not been developed. You are encouraged to test each policy thoroughly before turning it on, but it becomes especially important in policies that have such a broad scope. The image below shows a policy that has already been tested and is ready to turn on. Policy enforcement will begin once it takes effect, usually within an hour or so after it has been created.



2.1.5.2. Create the policy

After you test the policy, you have one last opportunity to review and edit your settings. The image below summarizes the results of configuring the policy named U.K. Financial Data that started with the U.K. Financial Data DLP policy template and was customized in the previous steps. Anything configured during the previous steps can be revisited by clicking on Edit in the appropriate section.



2.1.6. Prepare Endpoint DLP

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items on Windows devices. Once devices are onboarded into the Microsoft 365 compliance center, the information about what activities (like copying to USB devices or printing) users perform on sensitive items is visible to those who have access to activity explorer in the Microsoft 365 compliance center. You can also take the extra step of auditing or restricting those activities via data loss prevention policies.

This unit walks you through the additional steps required to use Endpoint DLP:

- Confirm your devices meet requirements
- Onboard devices
- Configure global Endpoint DLP settings

2.1.6.1. Confirm devices meet requirements

Windows devices that you plan on monitoring with Endpoint DLP must meet the system requirements. Review the requirements before you onboard devices.

2.1.6.2. Onboard devices

Before you can include Windows devices in DLP policies, you need to *onboard* them, or enable data collection.

To enable data collection from a device, the account onboarding the device must be a member of any of these roles:

- Global admin
- Security admin
- Compliance admin

Use the following steps to add an account to a role:

- In the Microsoft 365 admin center, select **Roles**.
- In the **Azure AD** tab, select **Show all roles**.
- Select one of the roles and add the user account.

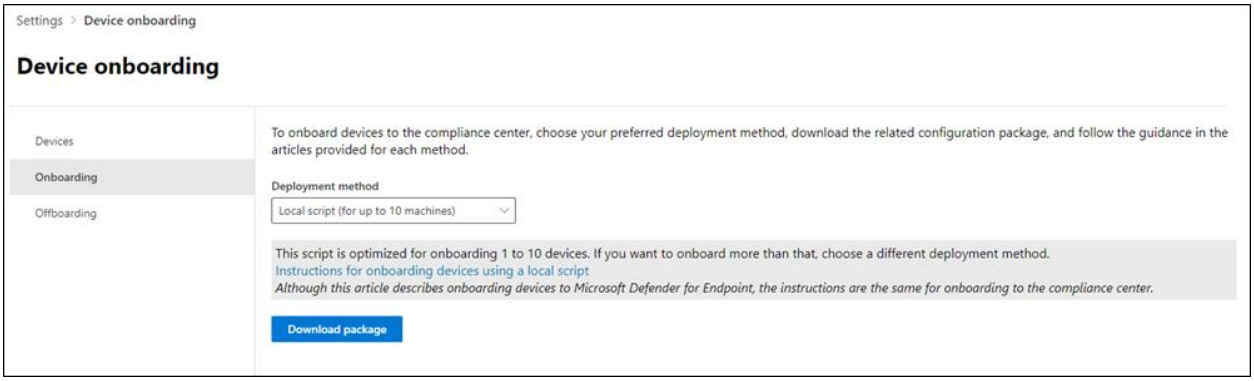
Give users only the access they need by assigning the least-permissive role.

2.1.7. Onboarding options

Onboarding and offboarding are handled via scripts you download from the **Device onboarding** center. The center has custom scripts for each of these deployment methods:

- Local script (up to 10 machines)
- Group policy
- Microsoft Endpoint Configuration Manager
- Mobile Device Management/Microsoft Intune
- VDI onboarding scripts for non-persistent machines

In the Microsoft 365 compliance center, select **Settings**, then select **Device Onboarding** to view a list of monitored devices and download the packages used to onboard or offboard devices using your preferred deployment method.



2.1.7.1.1. Onboarding using local script

We'll use the *Local script (for up to 10 machines)* script to onboard devices. The local script is meant for testing purposes - you can see how Endpoint DLP will affect your devices and environments before you roll it out in your production environment.

Here are the instructions for onboarding a Windows device using a local script.

- On the **Device onboarding** page in the compliance center, select **Onboarding**.
- Select **Local script (for up to 10 machines)** under **Deployment method**.
- Select **Download package**, and then save the DeviceComplianceOnboardingPackage.zip file.
- Extract the DeviceComplianceOnboardingPackage.zip file to a location accessible from the device you want to onboard, like a network share or the local device's Desktop. (You may need to bypass any messages or errors stating that downloading the file may harm your device and is not safe.)
- In the Windows Explorer or wherever you extracted the files, right-click **DeviceComplianceLocalOnboardingScript.cmd**, then select **Run as Administrator**.
- If a **User Account Control** window appears, select **Yes**.
- Follow the prompts on the screen to onboard the device.

2.1.7.2. Configure global Endpoint DLP settings

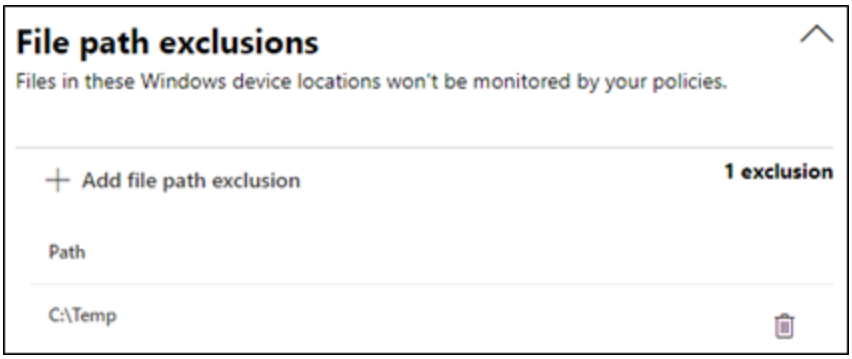
Global Endpoint DLP settings apply to all existing and new DLP policies that protect content on Windows devices. But these settings only apply to content impacted by DLP policies, not every item in, for example, the user's Documents folder.

In the Microsoft 365 compliance center left menu, go to **Data loss prevention** > **Endpoint DLP settings** to configure global settings.

Here are the settings available to you:

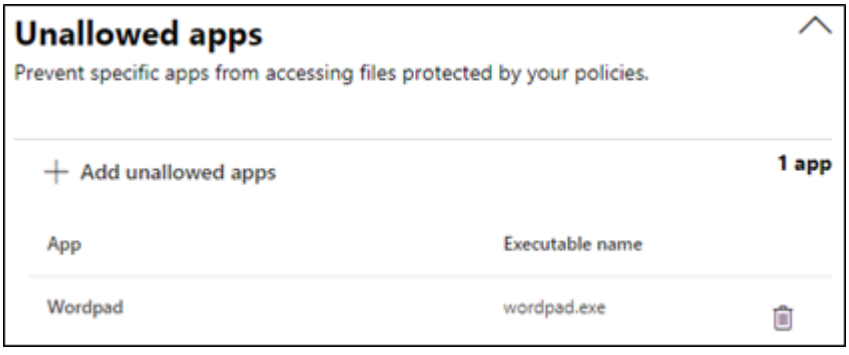
2.1.7.2.1. File path exclusions

Exclude specific paths from DLP monitoring, alerting, and policy enforcement. Use the setting for file paths that are too active or that don't contain files you want to protect. You can use wildcards, system variables, and other options to refine which file paths you include or exclude. You can see in the following image an exclusion for the `C:\Temp` folder and all subfolders. All other folders on the device will be monitored.

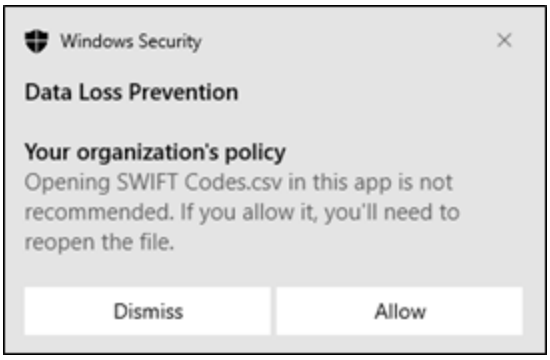


2.1.7.2.2. Unallowed apps

Prevent specific applications from accessing files protected by your policies. You can use the **Access by unallowed apps** setting to define what happens when one of your users tries to access protected data by using one of the specified apps. You can choose to allow the activity, allow but audit, block, or block the activity but let the user override the restriction. In this example, we've blocked Microsoft WordPad from opening any file that is protected by DLP policy. Other apps, like Microsoft Word, can open the same file.

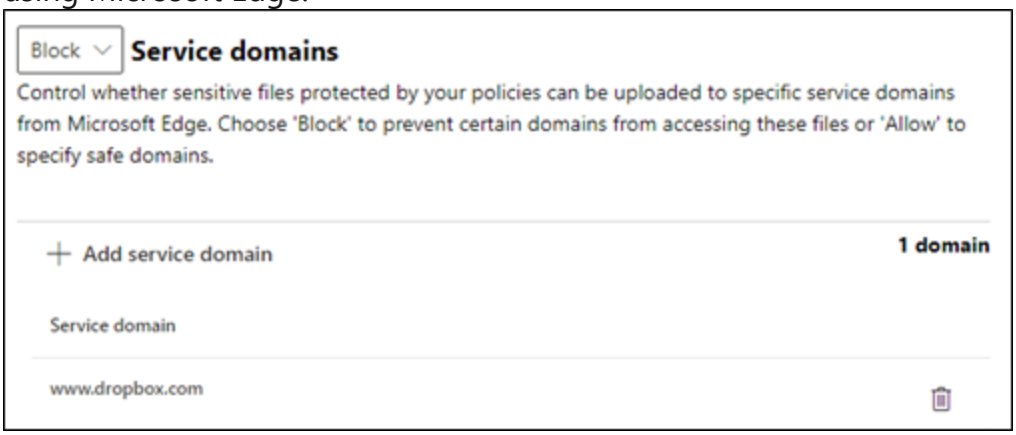


The following image shows a notification a user will see when they try to access the data with WordPad. The app isn't entirely blocked, so the user can select **Allow** to override the policy.

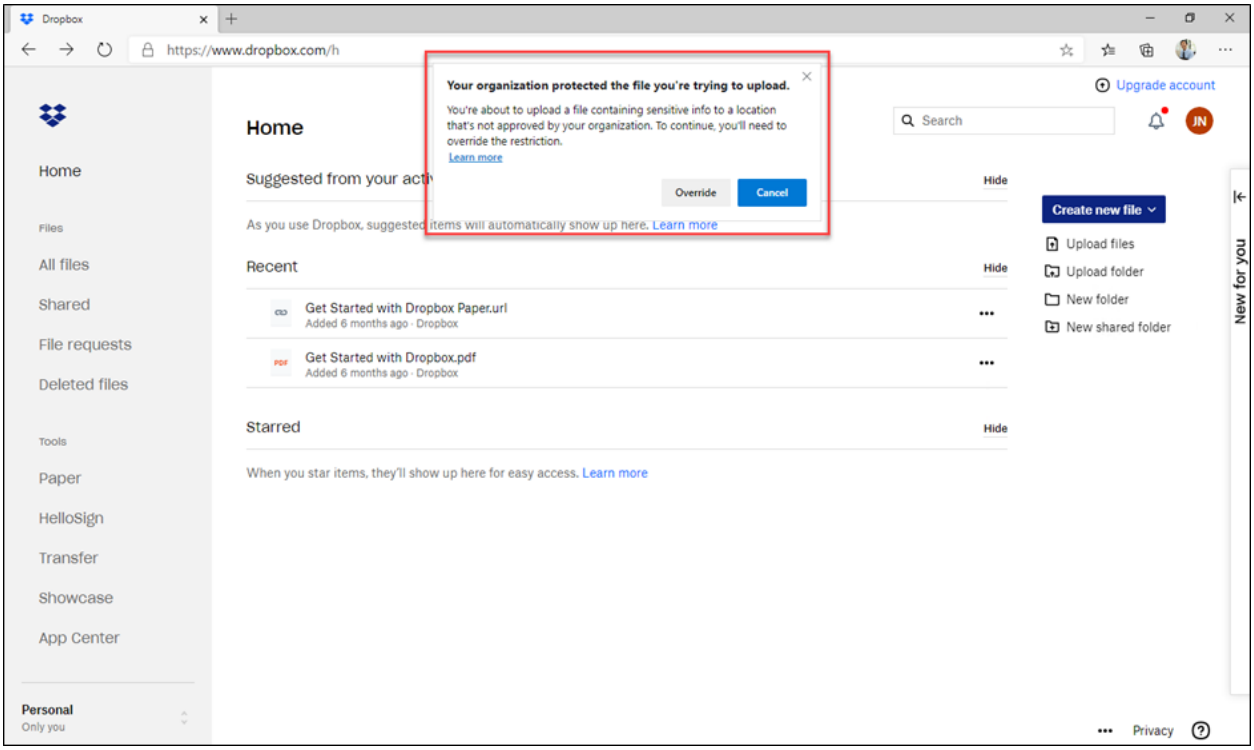


2.1.7.2.3. Service domain restrictions

Even if you've prevented all unsupported browsers from accessing sensitive data, sometimes you might also want to block supported browsers, like Microsoft Edge, from uploading protected content to specific web services. Service domain restrictions control whether sensitive files protected by your policies are allowed or blocked from accessing specific service domains from Microsoft Edge. Choose Block to prevent certain domains from accessing these files or Allow to specify safe domains. For example, the setting in the image below blocks users from uploading protected content to Dropbox even when using Microsoft Edge.



This is the notification that a user gets when they try to upload protected content into Dropbox. Notice that the user can override the restriction because the policy was configured with the option to allow override. The policy could as easily have been configured to prevent it from being overridden.



Note

Unless you've added other browsers to the **Unallowed browsers** list, user can still upload the protected content by using a different browser. Be sure to add the other browsers in use in your organization to the unallowed browsers list if you want service domain restrictions to work correctly.

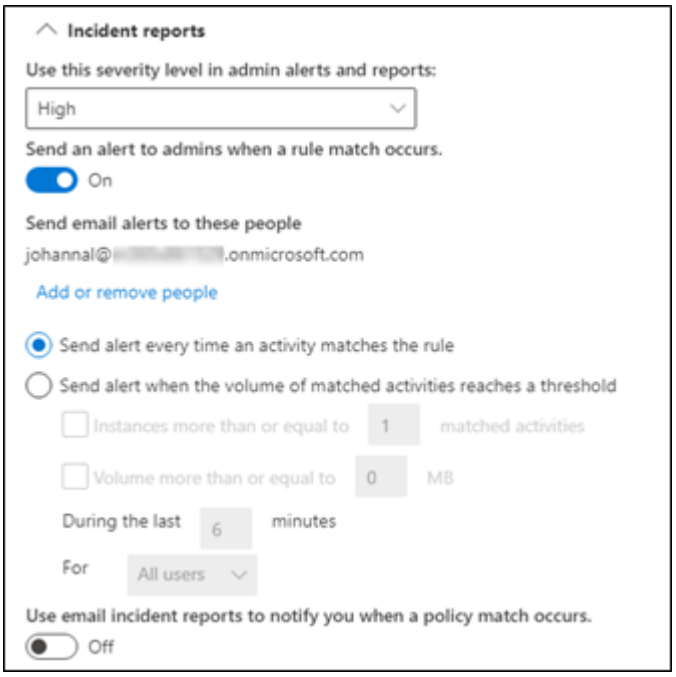
2.1.8. Manage DLP alerts in the Microsoft 365 compliance center

As noted earlier, part of the DLP policy creation process involves determining if you want to notify anyone when policies are triggered. You make those choices for each DLP policy rule you create. These alerts are displayed in the DLP Alerts (preview) dashboard and are governed by settings you configure in the Incident reports section of each data loss prevention policy rule. You can use the dashboard to both view and manage alerts.

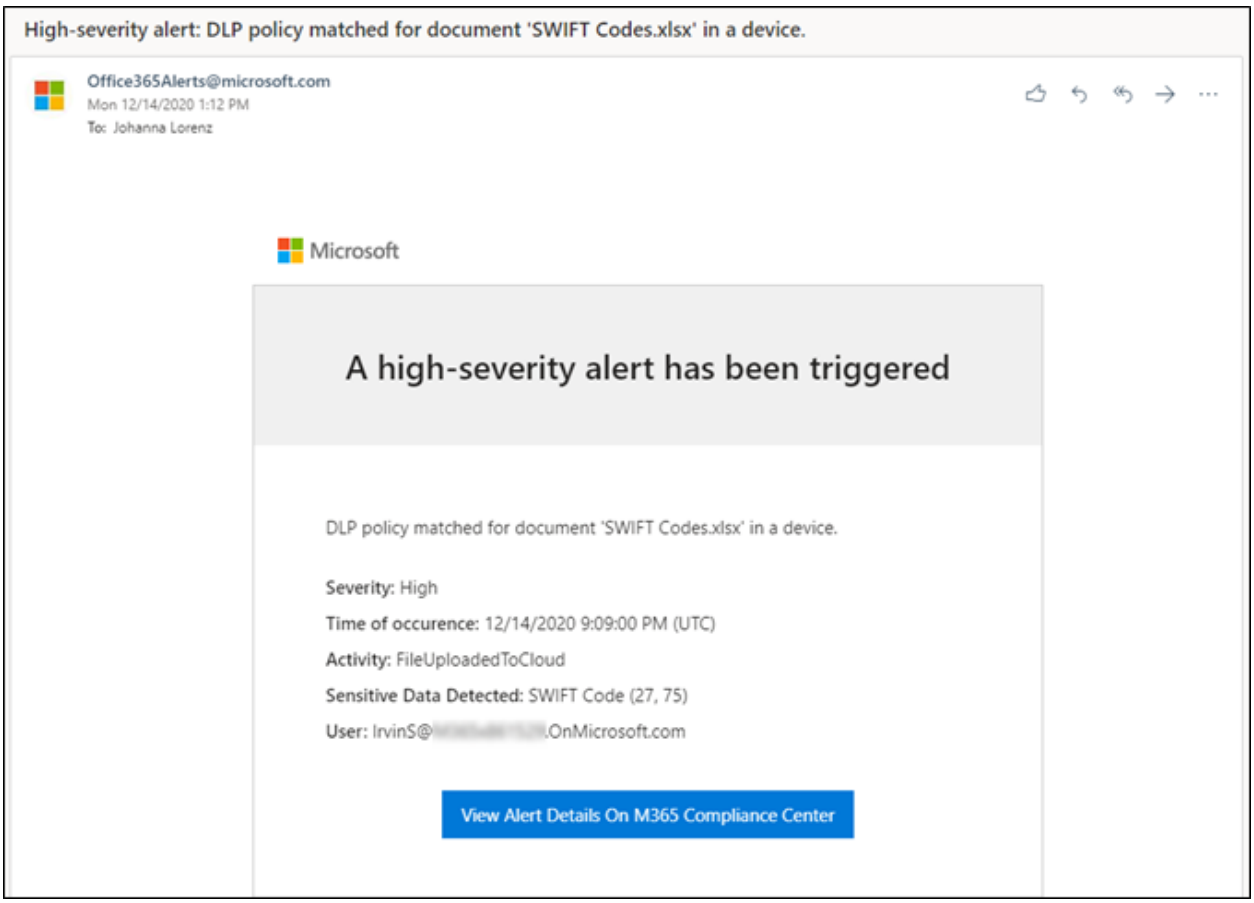
You have flexibility in defining when alerts are sent. One option is to send an alert every time an activity matches the rule. A second option is to only send the alert when a threshold, like the number of times the policy was violated, or the volume of data reaches a specific threshold.

The image below shows the portion of the DLP policy rule configuration process where you specify incident reports. The configuration below sends an email

to `johannal@<tenant>.onmicrosoft.com` and adds an alert to the DLP Alerts (preview) dashboard. Anyone with the rights to view DLP alerts will see the alert on the dashboard. Only the user(s) listed under Send and alert to admins when a rule match occurs will receive the email.

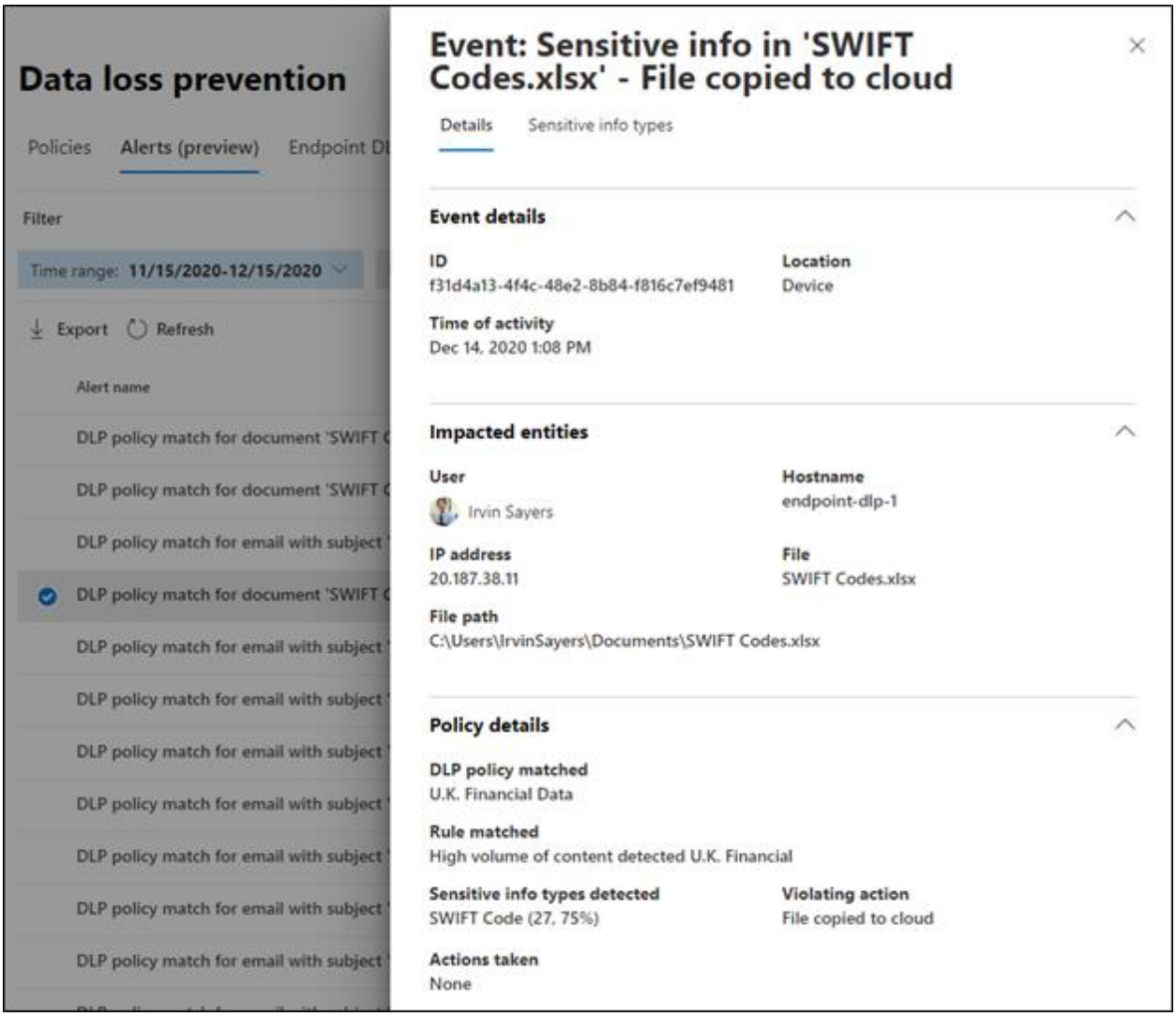


The image below shows the body of an email produced and sent to `johannal@<tenant>.onmicrosoft.com` when the high-severity alert has been triggered based on the configuration above. In this case, the activity that triggered the high-severity alert was a DLP policy that included a rule with an endpoint DLP setting to trigger enforcement when content containing sensitive data was uploaded to the cloud.



When you click **View Alert Details** in the notification, you see the DLP Alerts (preview) view in the compliance center. Select the event that prompted the alert. (You can also get to the alerts by going to **Data loss prevention** > **Alerts (preview).**)

In this case, we see that the event was a file that included a high volume of U.K. financial data was copied to the cloud. While not shown in the image below, the administrator can initiate a workflow to manage each alert to resolution and/or send an email to another user informing them of the DLP policy violation.



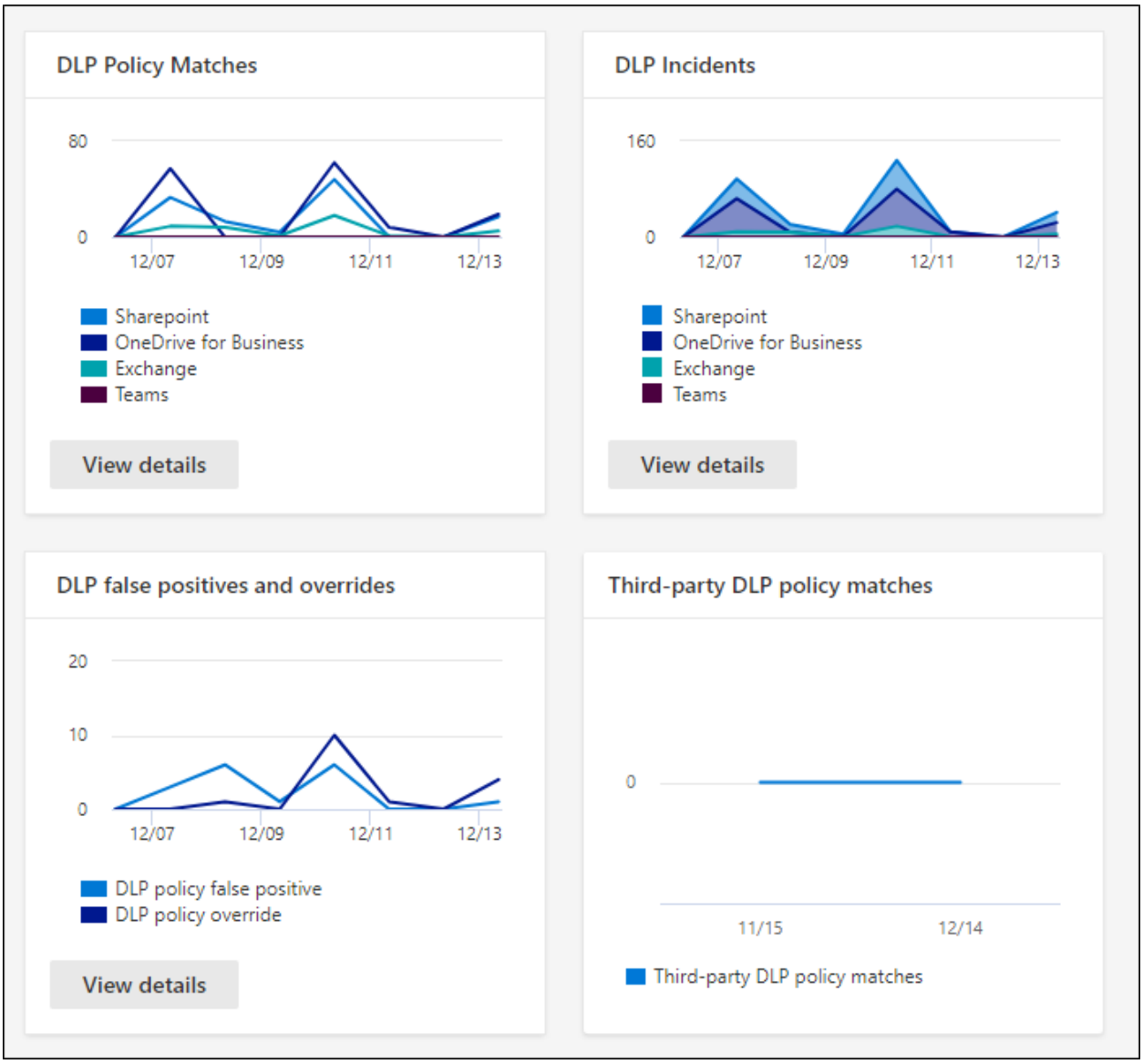
2.1.9. View data loss prevention reports

The DLP-specific reports available in the Microsoft 365 compliance center include:

- DLP policy matches
- DLP incidents
- DLP false positives and overrides
- Third-party DLP policy matched

Navigate to **Microsoft 365 compliance center > Reports** to view the reports.

The image below shows the summary cards for the reports in the Microsoft 365 compliance center.



Click **View details** to see the data in each report.

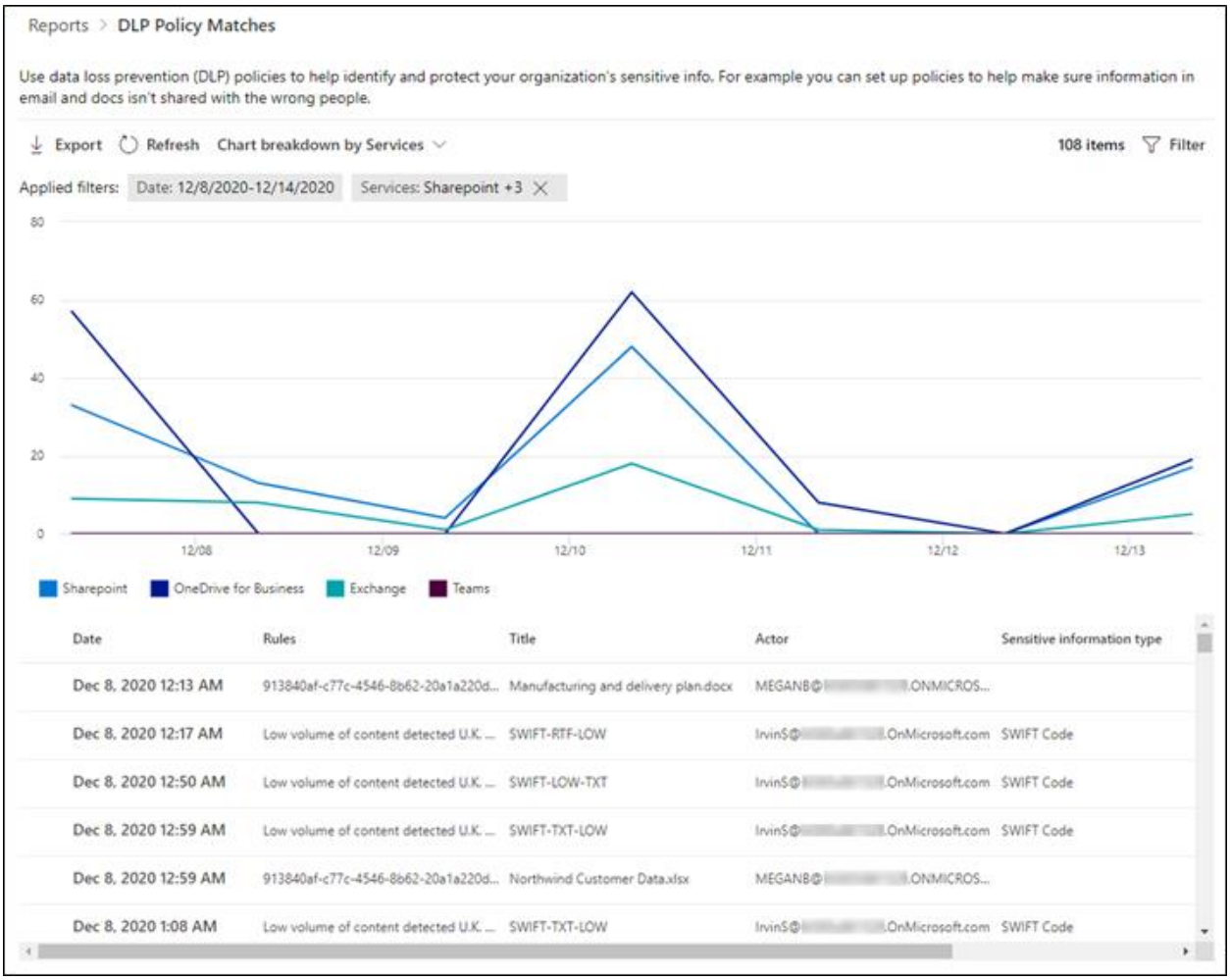
2.1.9.1. DLP policy matches

The DLP policy matches report shows the count of DLP policy matches over time. You can filter the report by date, location, policy, or action. You can use this report to:

- Tune or refine your DLP policies as you run them in test mode. You can view the specific rule that matched the content.
- Focus on specific time periods and understand the reasons for spikes and trends.
- Discover business processes that violate your organization's DLP policies.

- Understand the business impact of the DLP policies by viewing what actions are being applied to content.
- Verify compliance with a specific DLP policy by showing any matches for that policy.

This image shows the DLP policy matches report, sorted by services. (You can also choose to sort by policies or by action.)



2.1.9.2. DLP incidents

Like the policy matches report, the DLP incidents report shows policy matches over time, but in a different way - at the rule level. If an email matched three different rules, the DLP policy matches report shows three different line items. By contrast, the DLP incidents report shows matches at the item level: if an email matched three different rules, the incidents report shows a single line item for that item.

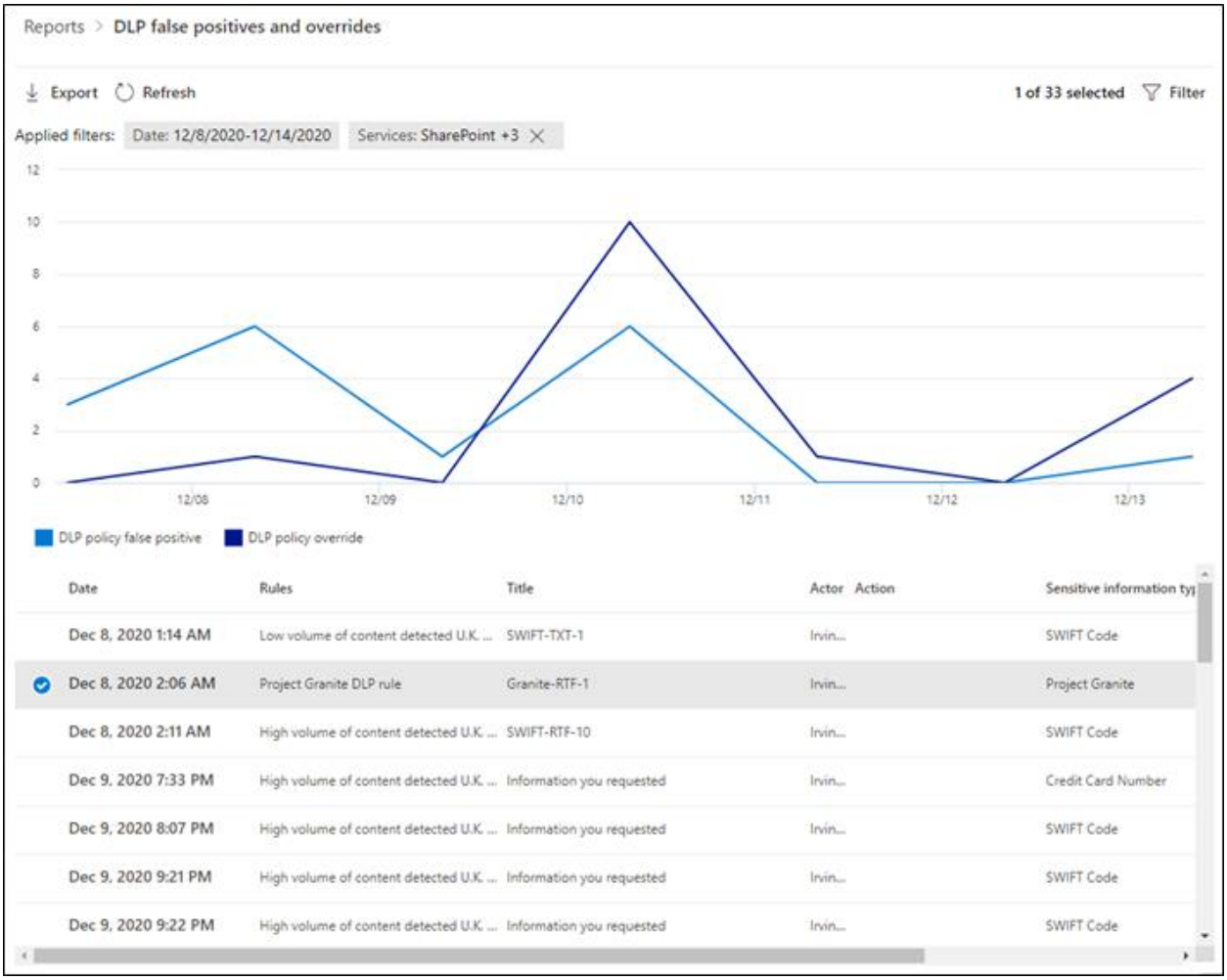
Because the report counts are aggregated differently, the DLP policy matches report is better for identifying matches with specific rules and fine-tuning DLP policies. The DLP incidents report is better for identifying specific content causing issues with DLP policies.

2.1.9.3. DLP false positives and overrides

The DLP false positives and overrides shows a count of policy overrides and false positive over time. You can filter the report by date, location, or policy. You can use this report to:

- Tune or refine your DLP policies by seeing which policies incur a high number of false positives.
- View the justifications submitted by users when they resolve a policy tip by overriding the policy.
- Discover where DLP policies conflict with valid business processes by incurring a high number of user overrides.

This image shows the DLP false positives and overrides report. One line in the chart shows false positives and the other shows policy overrides over time. Below the line chart is a list of individual items resulting in false positives and overrides. You can click on each item to examine it further; for example, to see the justification provided for a policy override.



2.1.10. Knowledge check

2.1.10.1. Question

1. A user sends an email to several recipients containing 16 unique credit card numbers that match a single DLP Policy rule with this sensitive information type. How many lines will display on the DLP Policy matches report?

- 1
- 3
- 16

2.1.10.1.1. Correct Answer

- 1

Correct. The DLP policy matches report shows matches at a rule level. If an email matched three different rules, the DLP policy matches report would show three different

line items. By contrast, the DLP incidents report shows matches at an item level. If an email matched three different rules, the incidents report shows a single line-item for that item.

2.1.10.1.2. Wrong Answer

- 3

Sorry, this is incorrect. The DLP policy matches report shows matches at a rule level. If an email matched three different rules, the DLP policy matches report would show three different line items. By contrast, the DLP incidents report shows matches at an item level. If an email matched three different rules, the incidents report shows a single line-item for that item.

- 16

Sorry, this is incorrect. The DLP policy matches report shows matches at a rule level. If an email matched three different rules, the DLP policy matches report would show three different line items. By contrast, the DLP incidents report shows matches at an item level. If an email matched three different rules, the incidents report shows a single line-item for that item.

2.1.10.2. Question

2. Too many DLP policy false positives can have a negative effect on business production. Additionally, too many false positives can result in security teams ignoring the warnings. Microsoft sensitive information types are thoroughly tested. There is still a chance your organization may have specific needs not met by built-in sensitive information types. What do you do if your DLP incident report returns too many false positives?

- Modify the DLP policy.
- Create a new retention policy and attach it to the DLP policy.
- Design a new DLP policy.

2.1.10.2.1. Correct Answer

- Modify the DLP policy.

Correct. When identifying information to protect, you need to configure the conditions that will result in a policy being triggered via rules. Data loss prevention includes policy templates that include rules for detecting many common sensitive information types. You can modify these rules using the rule editor if they are resulting in too many false positives.

2.1.10.2.2. Wrong Answer

- Create a new retention policy and attach it to the DLP policy.

Sorry, this is incorrect. Retention policies are used to decide proactively whether to retain content, delete content, or both. They have nothing to do with data loss prevention.

- Design a new DLP policy.

While you certainly can design a new policy, modifying the existing policy is the best practice.

2.1.10.3. Question

3. Maintaining patient privacy is a top priority in the Health Care industry. As a senior care facility, what best practice should you employ using the ready-to-use U.S personal information policy template?

- Create a custom policy to identify HIPAA-protected information.
- Turn on the policy right away.
- Test the policy before releasing it.

2.1.10.3.1. Correct Answer

- Test the policy before releasing it.

Correct. In most cases, you will want to test the DLP policy to make sure it is functioning as expected and meets your specific organization's needs.

2.1.10.3.2. Wrong Answer

- Create a custom policy to identify HIPAA-protected information.

Sorry, this is incorrect. Microsoft data loss prevention policy templates are thoroughly tested. Create a custom policy only if none of the built-in policies meet your requirements.

- Turn on the policy right away.

Sorry, this is incorrect. It's always a good practice to test the DLP policy first to validate functionality and alignment with your specific organizational needs.

2.1.10.4. Question

4. You have already deployed data loss prevention and are using it to protect data in Microsoft Teams, Exchange, SharePoint, and OneDrive. You also want to protect data stored on your Windows devices, so you have modified an existing policy and added Devices to the list of locations you will protect. What else must you do to begin protecting content on your Windows devices?

- Make sure each device is Azure AD registered.
- Onboard each device.
- Once created, you can't add locations to a DLP policy, so this isn't a valid scenario.

2.1.10.4.1. Correct Answer

- Onboard each device.

Correct. Device onboarding enables collecting data from devices to incorporate into Endpoint DLP. Only devices that have been onboarded can be included in DLP policies that target Windows devices.

2.1.10.4.2. Wrong Answer

- Make sure each device is Azure AD registered.

Sorry, this is incorrect. Each device that will be protected must be Azure AD joined or Hybrid Azure AD joined. Azure AD registered devices are not supported.

- Once created, you can't add locations to a DLP policy, so this isn't a valid scenario.

Sorry, this is incorrect. Locations can be added or removed from DLP policies.

2.2.Configure DLP policies for Microsoft Cloud App Security and Power Platform

2.2.1. Introduction

Your organization's data is likely one of the most important assets you're responsible for safeguarding as an administrator. The ability to build apps and automation to use that data is a large part of your company's success. You can use Power Apps and Power Automate for rapid build and rollout of these high-value apps so that users can measure and act on the data in real time.

You can use DLP policies to non-Microsoft cloud apps to monitor and detect when sensitive items are used and shared via non-Microsoft cloud apps. Using these policies provides you the visibility and control you need to ensure that they're correctly used and protected.

In this module you will learn how to discover, classify, and protect sensitive and business-critical content throughout its lifecycle in Power Platform and Microsoft Cloud App Security protected applications and make decisions about policy priority.

2.2.1.1. Learning objectives

In this module, you will be able to:

- Configure data loss prevention policy and rule priorities
- Implement DLP policies in test mode
- Configure Data loss prevention policies in PowerPlatform
- Integrate DLP Policies into MCAS for advanced functionality

2.2.1.2. Prerequisites

- Basic knowledge of data loss prevention in Microsoft 365
- Basic knowledge of Microsoft Cloud App Security
- Basic knowledge of Power Platform

2.2.2. Configure DLP policies for Power Platform

While DLP policies in the Microsoft 365 Compliance center protect data in Microsoft 365 services from being shared, DLP policies in Power Platform are used to restrict the communication between connectors. A connector in Power Platform is a wrapper or an API that allows predefined triggers and actions to access the data behind it.

There are three groups you can use to categorize your connectors:

CONFIGURE DLP POLICIES FOR POWER PLATFORM

Category	Actions
Business	Allows connections only to other connectors in the business group
Non-Business	Allows connections only to other connectors in the non-business group
Blocked	Blocks any connection attempts to these connectors

Connectors can reside in only one group at a time. For example, the SharePoint Online connector can only be part of the business group or the non-business group and not both at the same time. By moving the SharePoint Online and another 3rd party connector to the Business group, you're preventing users from creating flows and apps that combine these two connectors with any of the connectors in the Non-Business or Blocked groups without affecting the existing workflows that use both SharePoint Online connectors.

There is no specification as to the type of data you can share over the connector. For example, if you access a SharePoint Online connector you can access the content of a library no matter what is placed in that library.

To protect data in your organization, you can use PowerApps to create and enforce policies that define the consumer connectors for which specific business data can be shared. These DLP policies ensure that data is managed in a uniform manner across your organization, and they prevent important business data from being accidentally published to connectors such as social media sites.

While the blocked group exists, not all Connectors can be added to the blocked group. In this case the Block action will be greyed, and a warning will appear.

Note

If you select the blocked group as default, all new blockable connectors will be blocked by default and unblockable connectors will be added to the non-business group.

An environment is a space to store, manage, and share your organization's business data, apps, and flows. It also serves as a container to separate apps that may have different roles, security requirements, or target audiences.

Tenant-level policies can be defined to include or exclude specific environments. To follow the steps described here for tenant-level policies, one of the following permissions is required:

- Power Platform admin permissions
- Microsoft 365 Global admin permissions

To create environment-level policies, you need to have Power Apps Environment Admin permissions.

If you want to create a DLP Policy to deny connectivity between SharePoint Online and non-business apps using Power Platform admin center, follow these steps:

1. In Power Platform admin center, select **Data policies**, and then select **+ New policy**.
2. Enter a policy name, and then select **Next**.
3. Review the various attributes and settings you can make on the **Assign Connectors** page.
4. Select **SharePoint** connector, and then select **Move to Business** button from the top menu bar. You can also use the ellipsis (three dots) to the right of the connector name.
5. After you've completed all the connector assignment across the **Business**/**Non-Business**/**Blocked** groups, select **Next**.
6. On the Define scope page, you can choose the environments to add to this policy. Select **Exclude certain environments** and select **Next**.
7. On the **Add Environments** page, for tenant-level policies, the list will show the tenant-level admin all the environments in the tenant. For environment-level policies, this list will only show the subset of environments in the tenant that are managed by the user who has signed in as an environment admin. Select the environments you want to include in the policy and add them to the policy scope by using **Add to policy** from the top menu bar. Then select **Next**.
8. On the Review and create policy page you can review all settings. Select **Create Policy**.

Or you can use the PowerApps PowerShell module using the **New-DlpPolicy** cmdlet to create a DLP policy for Power Platform.

2.2.3. Combine DLP with Microsoft Cloud App Security

Data loss prevention (DLP) policies can be used for non-Microsoft cloud apps as part of the Microsoft 365 DLP suite of features.

You can use DLP policies for non-Microsoft cloud apps to monitor and detect when sensitive data is used and shared via non-Microsoft cloud apps. Using these policies provides visibility and control that helps prevent risky behavior.

You can create DLP policies for non-Microsoft cloud apps in two ways:

- Create file policies in the cloud app security portal
- Create DLP policies in the Compliance center and specify Microsoft cloud app security as the location

File policies allow control of the actions you can execute in MCAS when a policy match is found. Whereas DLP policies allow you more control over non-Microsoft cloud apps. If you want more control over the SharePoint Online and OneDrive for Business cloud apps you should use the SharePoint Online or OneDrive for Business portals.

You may need to activate the file monitoring in MCAS before creating file policies. Perform the following steps to enable MCAS to see files in the SaaS apps:

1. Navigate to the **Cloud App Security** portal at https://portal.cloudappsecurity.com.
2. Select the cogwheel in the upper right and select **Settings**.
3. Select **Files** from the **Information Protection** section.
4. Check **Enable file monitoring** if not checked already and select **Save**.

After selecting this setting, you can create file policies in MCAS.

To use the capabilities of the Compliance center to monitor non-Microsoft cloud apps you need to connect these apps to Microsoft Cloud App Security. Afterwards they will be available as instances in the Microsoft Cloud app security location of your DLP policies. This is required to complete integration of MCAS into DLP.

If you do not select a specific instance the policy will apply to all connected apps.

When you create a rule in the DLP policy, you can select an action for non-Microsoft cloud apps. To restrict these apps, select **Restrict Third Party Apps**. You can choose various actions for every supported non-Microsoft cloud app. For every app, there are different possible actions depending on the cloud app API.

2.2.4. Configure file policies in Microsoft Cloud App Security

Microsoft Cloud App Security (MCAS) built-in DLP engine performs content inspection by extracting text from all common file types (100+) including Office, Open Office, compressed files, various rich text formats, XML, HTML, and more.

The engine combines three aspects under each policy:

- Content scan based on preset templates or custom expressions.
- Context filters including user roles, file metadata, sharing level, organizational group integration, collaboration context, and additional customizable attributes.
- Automated actions for governance and remediation.

Once enabled, the policy continuously scans your cloud environment and identifies files that match the content and context filters and applies the requested automated actions. These policies detect and remediate any violations for at-rest information or when new content is created. Policies can be monitored using real-time alerts or using console-generated reports.

The other option is to leverage the Data Classification Service that is also employed by the DLP policies configured in the Compliance center. You can use this option to have a uniform experience across all your configured DLP policies.

2.2.4.1. Creating a new file policy

To create a file policy, follow this procedure:

1. In the Cloud App Security portal at https://portal.cloudappsecurity.com, select Control followed by Policies.
2. Select Create policy and select File policy.
3. Give your policy a name and description, if you want you can base it on a template.
4. Give your policy a Policy severity. If you have set Cloud App Security to send you notifications on policy matches for a specific policy severity level, this level is used to determine whether the policy's matches trigger a notification.
5. Within Category, link the policy to the most appropriate risk type. This field is informative only and helps you search for specific policies and alerts later, based on risk type. The risk may already be preselected according to the category for which you chose to create the policy. By default, File policies are set to DLP.

6. Create a filter for the files this policy will act on to set which discovered apps trigger this policy. Narrow down the policy filters until you reach an accurate set of files you wish to act upon. Be as restrictive as possible to avoid false positives. For example, if you wish to remove public permissions, remember to add the Public filter, if you wish to remove an external user, use the "External" filter etc.
7. Under the first Apply to filter, select all files excluding selected folders or selected folders for Box, SharePoint, Dropbox, OneDrive, where you can enforce your file policy over all files on the app or on specific folders. You're redirected to sign-in to the cloud app, and then add the relevant folders.
8. Under the second Apply to filter, select either all file owners, file owners from selected user groups or all file owners excluding selected groups. Then select the relevant user groups to determine which users and groups should be included in the policy.
9. Select the content Inspection method. You can select either Built-in DLP or Data Classification Services.
10. Choose the Governance actions you want Cloud App Security to take when a match is detected and select Create Policy.

Once you've created your policy, you can view it in the **File policy** tab. You can edit a policy, calibrate its filters, or change the automated actions.

The policy is automatically enabled upon creation and starts scanning your cloud files immediately. Take extra care when you set governance actions, they could lead to irreversible loss of access permissions to your files.

It's recommended to narrow down the filters to exactly represent the files that you wish to act upon, using multiple search fields. The narrower the filters, the better. For guidance, you can use the **Edit and preview results** button in the Filters section.

Note

The Inspection method supports several built-in sensitive information types and custom expressions that can be substrings, exact string matches, and regular expressions, which are the most powerful method to find the targeted information. Creating and maintaining the correct regular expressions is a recurring task and more information can be found in the resource section of this module.

2.2.4.2. File policy matches

If you want to view all files that are suspected to violate a policy, follow these steps:

1. Select **Control** and then **Policies**.
2. Search the respective **File Policy** you want to view.
3. Select the three dots (**...**) on the right-side of the policy and select **View all matches**.
4. You will see a list of files that are currently recognized by the file policy to match the selected filters. You can use this view to see the impact your policy has before you change it to apply any Governance actions.

2.2.5. Manage DLP violations in Microsoft Cloud App Security

When you create a DLP policy using Microsoft Cloud App Security as a location in the Compliance Center, the matches will appear in the regular DLP reports.

When you create a file policy in MCAS the matched conditions and taken actions will instead be logged in MCAS.

For example, you created a file policy in MCAS to identify files including Tax Identification numbers which are shared with external users from OneDrive for Business or SharePoint Online and automatically move them into the trash folder and revoke external access. If you want to see any matches on this policy, open the Cloud app security portal and follow these steps:

1. Under Control, select **policies**.
2. Search for the policy you want to review.
3. Select **Open Matches** from the Count Column for the Policy you want to review.
4. You should see three tabs at the top of the page:
   4.1. Match now allows you to see currently existing matches for the file policy and use the filters at the top to refine the results.
   4.2. Quarantined allows you to see the files that have been quarantined because of a file policy governance action.
   4.3. History allows you to see former matches to the policy which have been resolved because of changes to the file or the policy itself.

Use this page to find patterns in your matches and decide if you need to take action. For example, you notice a high volume of matches, but they all originate from a single user. You should investigate the matches and identify if the user has a valid business reason to generate these matches.

2.2.6. Knowledge check

2.2.6.1. Question

1. Microsoft Cloud App Security (MCAS) built-in DLP engine performs content inspection by extracting text from all common file types including which of these file types?

- BTML
- All file types
- XML and HTML

2.2.6.1.1. Correct Answer

- XML and HTML

This answer is correct. These are two of the files types.

2.2.6.1.2. Wrong Answer

- BTML

This answer is not correct. This isn't one of the file types.

- All file types

This answer is not correct. Not all file types are inspected.

2.2.6.2. Question

2. Which type of DLP policy may be configured in the Microsoft 365 Compliance center?

- Exchange DLP policies
- PowerPlatform DLP policies
- Azure Information Protection policies

2.2.6.2.1. Correct Answer

- Exchange DLP policies

This answer is correct. Exchange Policies can be configured in the Microsoft 365 Compliance Center.

2.2.6.2.2. Wrong Answer

- PowerPlatform DLP policies

This answer is not correct. PowerPlatform DLP policies can only be configured in the PowerPlatform portal.

- Azure Information Protection policies

This answer is not correct. These policies are configured in Azure.

2.2.6.3. Question

3. How can a DLP policy for non-Microsoft cloud apps be configured?

- Policies may be created in the Microsoft Exchange Online portal.
- Policies can be created in the Microsoft cloud app security portal.
- Policies can be created in the Microsoft 365 Security portal.

2.2.6.3.1. Correct Answer

- Policies can be created in the Microsoft cloud app security portal.

This answer is correct. These policies are created in the Microsoft cloud app security portal.

2.2.6.3.2. Wrong Answer

- Policies may be created in the Microsoft Exchange Online portal.

This answer is not correct. These policies may not be created in the Exchange Online portal.

- Policies can be created in the Microsoft 365 Security portal.

This answer is not correct. These policies are not created in the Microsoft 365 security portal.

2.3.Manage data loss prevention policies and reports in Microsoft 365

2.3.1. Introduction

Ensuring that your DLP policies are processed in the correct order and that they are tested properly before activation is key to the success of your organization. Analyzing the performance of DLP policies can be done through dashboards in Microsoft 365.

Once your DLP policies are active, DLP reports display information about the behavior of DLP policies. They allow you to monitor and respond to unwanted sharing of sensitive data from your organization.

In this module, you will learn about the concept of policy precedence to ensure your policies are being processed according to your needs. You will also learn about DLP policy testing and how to respond to DLP incidents.

2.3.1.1. Learning objectives

After this module, you will be able to:

- Configure DLP for policy precedence
- Implement DLP policies in test mode
- Analyze DLP reports
- Manage permissions for DLP policy administration
- Monitor and respond to DLP policy violations

2.3.1.2. Prerequisites

- Knowledge of data loss prevention in Microsoft 365

2.3.2. Configure data loss prevention for policy precedence

DLP policies and rules contained within those policies **are processed in a specific order**. This process is called **policy precedence**. You can manually configure the order in which this rule will be selected for evaluation. The rules of DLP policy with the lowest order/priority number are processed first. By default, the first rule is configured as priority "0", the next one as "1", and so on.

All possible matches of policies are still recorded in the audit logs and visible in the DLP reports, even though only one DLP policy and their rule is enforced. DLP policies also provide an option to prevent processing of more policies when a match has been made.

The configured actions for certain condition matches can oppose each other. For example, you configure a DLP policy that blocks external sharing of personal data, without override allowed, and another policy for financial data, which allows override by end users. If only the last matching policy was applied, instead of taking the priority of a policy into account, then a user could hide personal data inside an email that also includes financial data and select the override encoded into the financial data policy to bypass the block action of the personal data policy. However, since the personal data policy should have a higher priority it will be applied instead.

2.3.2.1. Changing rule priority

If the financial data policy from the example above was ordered so a rule for a high volume of matches was prioritized below a rule for a low number of matches, even though a high number of matches is more restrictive, the user could still select the override that is allowed in the low matches rule and send out protected data. Even though both actions will be logged it could still take time to notice the behavior and take appropriate actions.

To change the order in which the DLP rules inside a policy are prioritized, you need the DLP Compliance Management role and follow these steps:

- In the Microsoft 365 Compliance Center, select **Policies**.
- Expand **Data** and select **Data loss prevention**.
- Select the policy you want to modify and select **edit policy**.
- Select **Next** twice to reach the **Customize Advanced DLP rules** dialog.
- Select **Edit** behind the name of the low volume rule you want to change in the priority order.
- Select a new priority number from the dropdown menu. You can select "0" to select the highest priority.
- You can also use PowerShell to change the priority of the DLP rule "Low Volume of Financial Data" to the highest value by using the following cmdlet:

```
Set-DLPComplianceRule -Identity "Low Volume of Financial Data" -Priority 0
```

2.3.2.2. Change policy priority

When you create more than one DLP policy, you can change the priority (or order). For example, if you have a personal data DLP policy and another financial data DLP policy and you want the personal data DLP policy to take precedence, follow these steps.

- In the Microsoft 365 Compliance Center, select **Policies** > **Data loss prevention**.

- Select the **three vertical dots** behind the name of the personal data policy.
- Select **Move to Top** to move the policy into the highest priority.
- You can also use PowerShell to change the priority of the DLP policy "EU Financial Data Policy" to the value 1 by using the following cmdlet:

```
Set-DLPCompliancePolicy -Identity "EU Financial Data Policy" -Priority 1
```

It is prudent to prioritize policies with less restrictive actions below more restrictive policies. Also, rules with less restrictive actions should be prioritized below more restrictive rules to prevent the less restrictive rules from overwriting any block actions of the more restrictive rules and policies.

2.3.3. Implement data loss prevention policies in test mode

When implementing DLP Policies, it can be difficult to determine their full impact on the users of your environment. Test mode exists so administrators can create new DLP Policies and monitor the impact and effectiveness of the policy to end users. The results will be delivered to you in the form of emails containing incident reports whenever a rule inside the policy matches content in the defined locations. Analyzing these reports will help you determine if the policy is functioning as intended or if you need to adjust the policy before activating it.

For example, you created a policy that protects German driver's license numbers from being shared but when checking the data classification specifications, you notice that the internal product numbers your company uses are similar to the pattern of the license numbers you want to protect. Before activating the policy, you want to test the impact it would have on user experience. To create the policy in test mode, you first need to start the usual creation process for a policy.

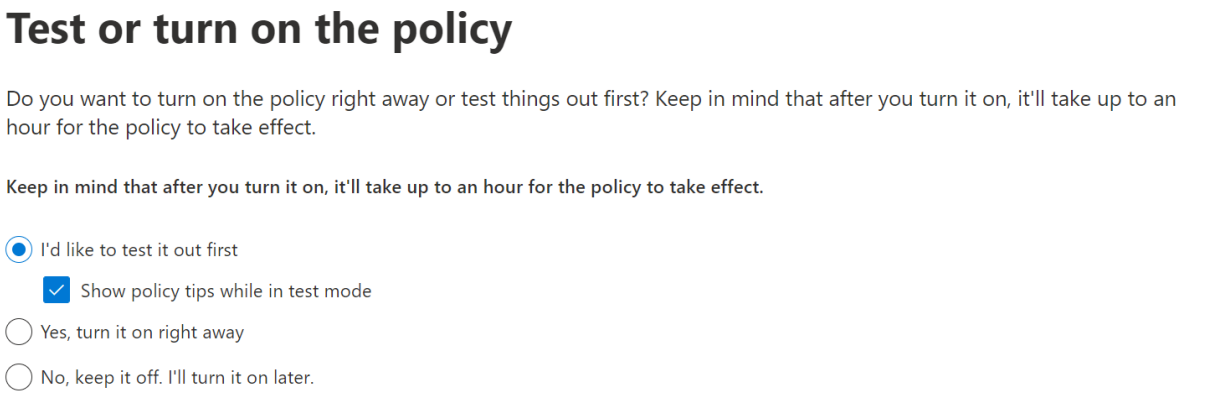
Next, determine if you want to inform users that they are about to share sensitive information. Test mode can be configured to be invisible or to display policy tips and send mails to end users. If the users are informed of the match, they can also review their content for sensitive information. This enables users to report false positives if they arise. False positives can occur when content matches a pattern it is not supposed to match. This active user feedback can be useful to increase the effectiveness of a DLP policy.

For example, a driver's license number and a phone number might have different patterns but there can still be a string of numbers that matches both patterns. DLP Policies not only match those patterns but also require other parameters to identify if the number is a driver's license or a phone number. A user might want to send their

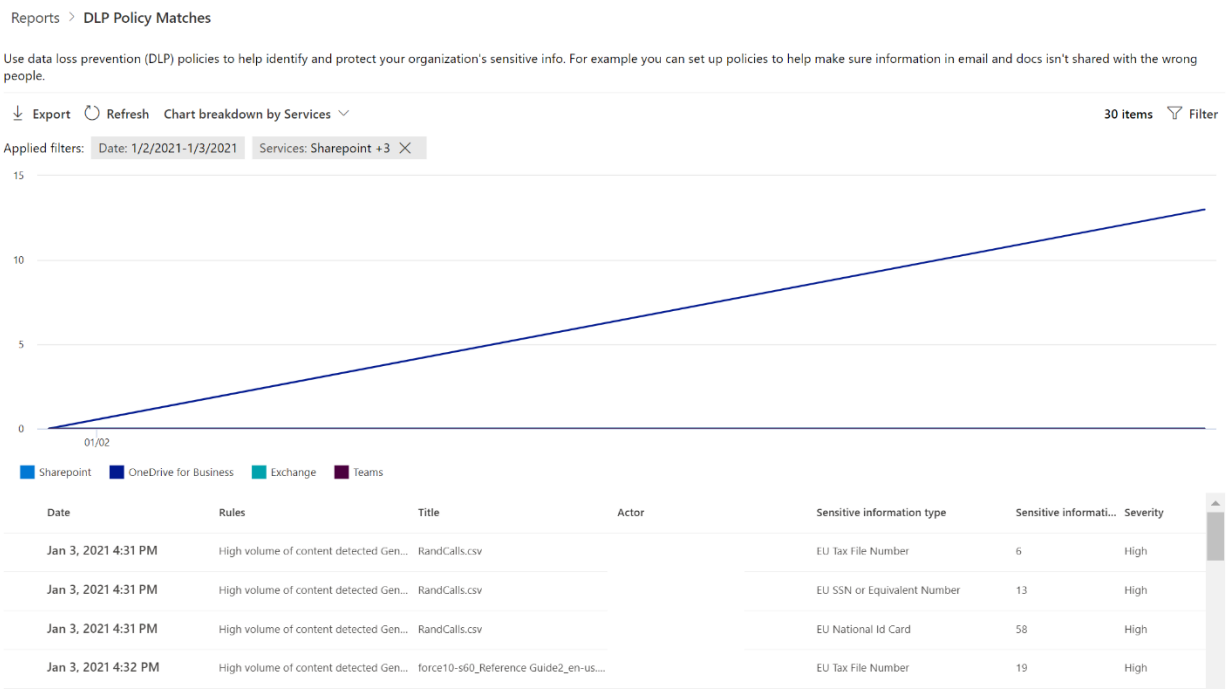
phone number to a customer, but the policy recognizes the driver's license pattern in proximity to a driver's license identifier, which would result in the user seeing a policy tip for your driver's license policy.

To enable test mode for your DLP policy, you need to edit the DLP policy and go to the **Test or turn on the policy** page, then follow these steps:

- Select **I'd like to test it out first**.
- If you want to show policy tips to your users, you can check **Show policy tips in test mode**, otherwise uncheck it.
- Select **Next** and review the policy.
- Select **Submit** after reviewing the policy.



- Next you can review the content your policy matches by utilizing the reports dashboard.
- In the Compliance Center, select **Reports** and then select **DLP policy matches**.
- On the Reports page, filter for the policy you created and review the results.



Tip

DLP Policy reports might take up to 24 hours to show up in your display!

Once you have seen the impact of a policy in the Reports Dashboard, you can modify the policy to adjust its sensitivity and add exceptions if you identify any words that consistently trigger false positives. For example, the frequent use of the word product number would indicate people are discussing a product number not a license number.

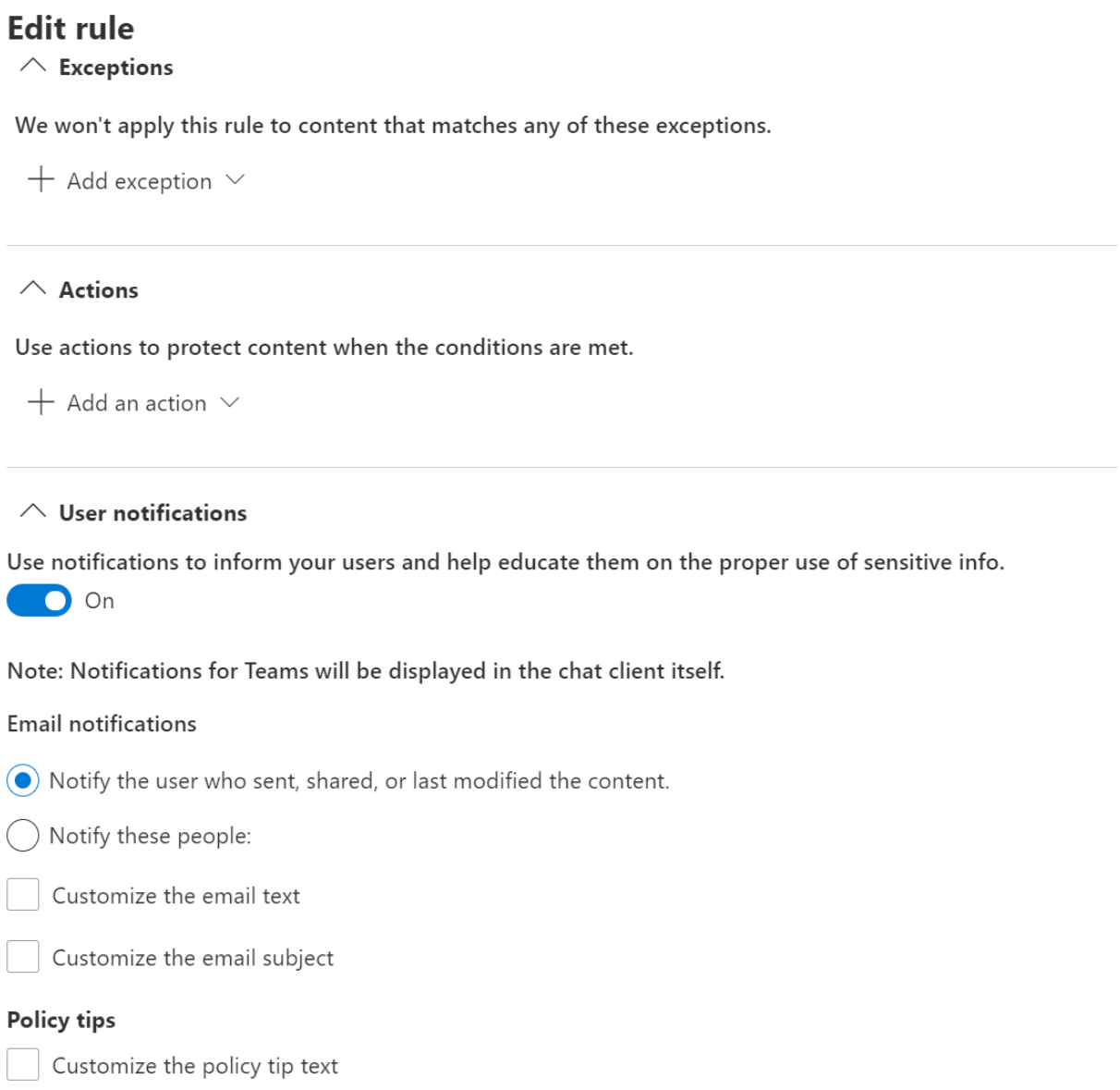
While a policy is implemented in test mode the actions are not executed. You can use exceptions to limit the number of false positives.

After you have monitored the alerts for some time and adjusted the sensitivity of your policy, you should keep the policy in test mode and activate the policy tips for some time. This will allow your users' time to help refine the policy further by reporting false positives.

2.3.3.1. Data loss prevention rule: user notifications

User notifications inform users that a policy was triggered. Enabling these notifications should get users' to report false positives so you can adjust policy sensitivity. You can enable User notification on DLP rules using the following steps:

1. Edit the DLP policy and go to the **Customize advanced DLP rules** pane.
2. Select **Edit** on the DLP rule you want to configure.
3. In **Edit rule** pane, go down to the **User notifications** section, in **Use notifications to inform your users and help educate them on the proper use of sensitive info**, select **On**.



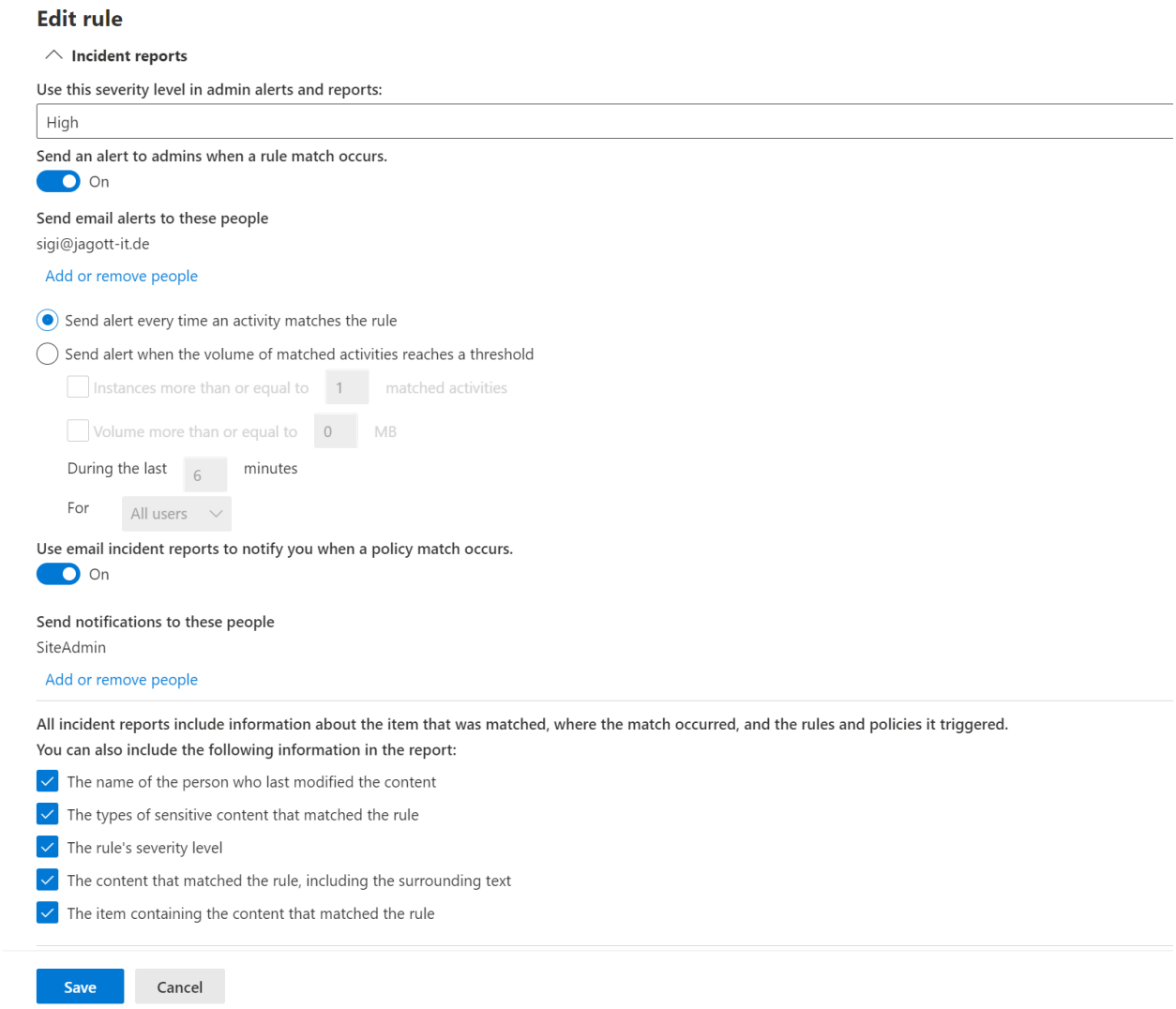
2.3.3.2. Data loss prevention rule: incident reports

When tuning policies in test mode you need to be informed about matches so you can adjust the sensitivity if matches are triggering a high number of false positives. In this

case, we are monitoring each rule inside the policy for itself and not a general policy match.

The following steps describe how to configure Incident reports in your DLP rules:

1. When creating the DLP rules for a policy, on the Edit rule pane, in Incident reports section, in Use this severity level in admin alerts and reports, select **Low/Medium/High** as your severity level.
2. If you want to get a notification email, select **Send alert to admins when a rule match occurs** and select your email address, and select **Send an alert every time an activity matches the rule**.
3. Decide on the various other parameters available to fine-tune your incident reports.



2.3.4. Explain data loss prevention reporting capabilities

After you create data loss prevention policies, administrators need to verify and monitor the performance of their DLP policies in production. This is an important recurring task for an organization to ensure they stay compliant with policies while minimizing impact on user productivity.

2.3.4.1. Data loss prevention reports in the Microsoft 365 compliance center

The Microsoft 365 compliance center provides the following DLP reports that can be accessed in reports under organization data:

1. DLP Policy Matches
2. DLP Incidents
3. DLP false positive overrides

The following table provides an overview for each DLP report.

DATA LOSS PREVENTION REPORTS IN THE MICROSOFT 365 COMPLIANCE CENTER

Report	Report contains...	Report is used for...	Recommendation
DLP Policy Matches	The count of DLP policy matches over time at a rule level, grouped by the available Microsoft 365 service locations. The report can be broken down by services, actions, or policies and get filtered by date, location, policy, or action.	Tune or refine your DLP policies as you run them in test mode. You can view the specific rule that matched the content.	The policy matches report is used for identifying matches with specific rules and fine-tuning DLP policies, to increase the accuracy of the policies matching a company's individual data shared regularly.
DLP Incidents	The count of DLP policy matches over time on item level, grouped by the available Microsoft 365 service locations. The report can be filtered by date,	Identify specific pieces of content that are problematic for your DLP policies.	The incidents report is used for identifying specific pieces of content that are problematic for your DLP policies and to identify groups of items that may require more protective actions.

DATA LOSS PREVENTION REPORTS IN THE MICROSOFT 365 COMPLIANCE CENTER

Report	Report contains...	Report is used for...	Recommendation
	location, policy, or action.		
DLP false positives and overrides	A count of user overrides and reported false positives. This report can be filtered by date, location, or policy.	Tune or refine your DLP policies by seeing which policies incur a high number of false positives.	The false positives and user overrides report should be used to identify the accuracy of the existing DLP policies, to be able to react fast when suddenly large numbers of faulty matches occur in a business impact.

All DLP reports can display data from the most recent four-month time period. The most recent data can take up to 24 hours to appear in the reports.

2.3.4.2. Data loss prevention alert management dashboard

Reports provide a quick overview of DLP events and can inform about an organization's trends. DLP policies can be configured to trigger an alert when the conditions are met. Use the incident report to investigate events.

The DLP alert management dashboard in the Microsoft 365 Compliance center can be used to show alerts of the following workloads:

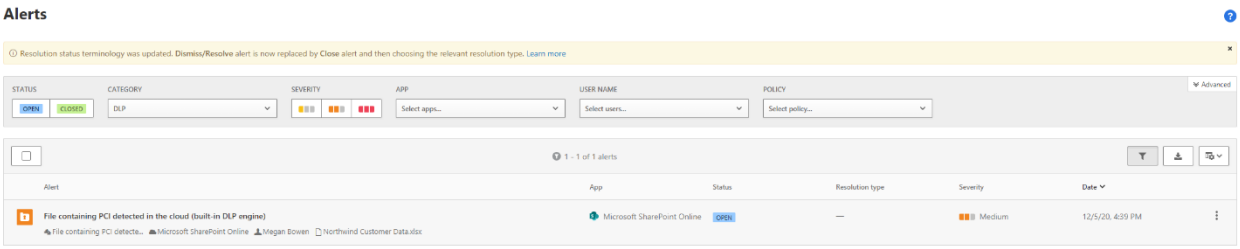
1. Exchange
2. SharePoint
3. OneDrive
4. Teams
5. Devices

The remediation of MCAS DLP alerts is done through the MCAS dashboard.

2.3.4.3. Data loss prevention alerts in the Microsoft Cloud App Security dashboard

You can also view a report for DLP alerts in the MCAS Dashboard. This report shows the alerts and matches of all your MCAS policies that are part of the DLP category. You can select each alert or match to gain information about:

1. The type of sensitive information
2. Location of the sensitive information
3. The policy creating the alert
4. The user triggering the policy match
5. The actions that have been taken to secure the matched file



Use the MCAS DLP alerts report to view an overview of MCAS policy alerts. Since policies created on the MCAS side have different options and scopes compared to MCAS policies created in the Compliance center, it's prudent to be aware of alerts in both dashboards.

2.3.5. Review and analyze data loss prevention reports

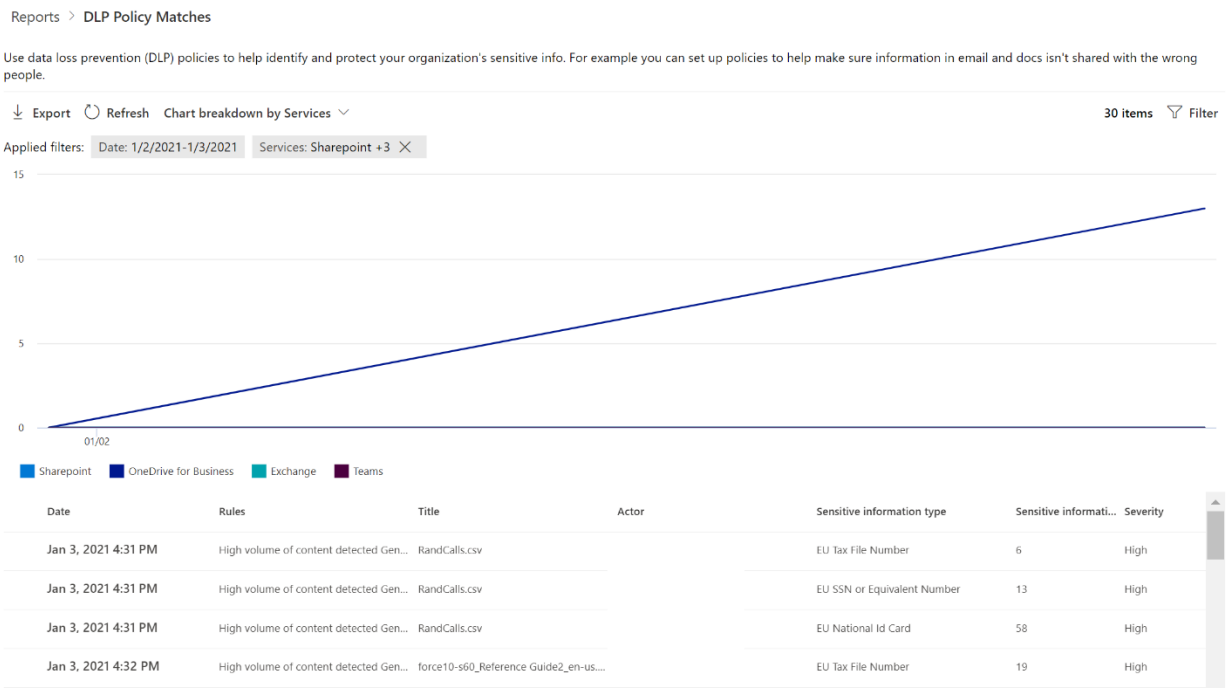
On the DLP Policy Matches report page and the DLP Incidents report page you will see a chart and a table displaying information about their respective occurrences. To analyze these DLP reports, you can break down the charts separated by either:

1. Affected service
2. Enforced action
3. Applied policy

Familiarizing yourself with the available filters and options of the DLP reports will help you fine-tune your policies and reduce false positives and overrides.

2.3.5.1. Review data loss prevention policy matches

When using the DLP policy matches report, you should use the filters to limit the report to specific policies. This will help you reduce the number of matches displayed and focus on the impact of selected policies in your organization.



Consider a scenario where you created a new policy to protect financial data a few days ago and currently have it set to test mode. You should set the start date in the filter close to the start date of the policy to avoid whitespace in your report from before the policy existed.

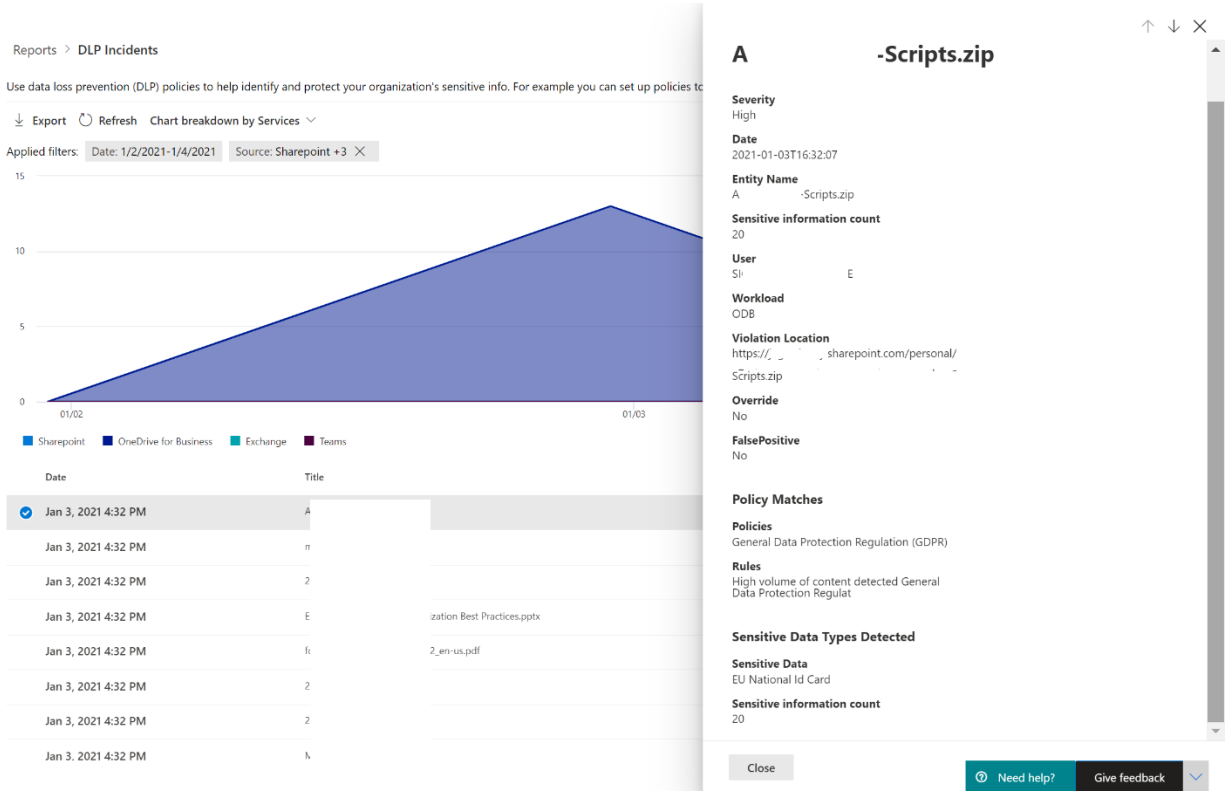
1. On the DLP Policy Matches page, in the right corner select **Filter**.
2. Select a Start date close to the creation date of the policy.
3. Under Services, make sure all services selected.
4. Under Policies, select the DLP policy you want to review in the dropdown menu.
5. Under Rules, select all rules and then select **Apply**.
6. To get a better understanding of how and where the policy will affect your users, you can use the dropdown menu at the top to change the breakdown of the chart:
7. Select **Chart breakdown by Services**.
8. In the dropdown menu, select **Chart breakdown by Action**.
9. Select one of the options from the legend to filter the results even more.

10. Use the table to view which rule matched and which sensitive information type is responsible for the match.
11. Switch between the breakdown options and modify the filters to identify peaks in specific services and times that could indicate a need to adjust your policy.
12. For example, a peak in the Exchange service for bank account numbers might indicate a leak, but it could also be the sign of a legitimate business process at odds with your new policy. Before adjusting the policy, you should investigate the situation.

2.3.5.2. Review data loss prevention incidents

When using the DLP Incidents report to get a general overview of which items generate many matches you should not limit the report to specific policies. This will allow you to identify items that fall under the scope of multiple policies and see which action is applied in the end.

Using the DLP incidents report you should keep the timeframe broad and drill-down if you identify any peaks at certain times.



For example, you created a new set of DLP policies and prioritized them according to your DLP strategy. If you want to see if the priority you chose aligns with the reality of

sensitive data in your organization, you should open the DLP incidents report page and follow these steps:

1. In the right corner select **Filter**.
2. Select a Start date and End date.
3. Under Services, make sure all services selected.
4. Select **All policies** in the dropdown menu.
5. Select **apply**.

If you see any high peaks use the start date and end date filters to limit the scope of the information to that peak. Look at the table and identify the items with the highest policy and rule counts to identify items that may be problematic for your policies. By selecting the item in the table, you can gain additional information about which rules and policies match the item. Review those rules and policies to see which actions should have been enforced according to your DLP strategy and verify that the correct actions have been enforced.

The DLP incidents report can not only be used to see items at odds with your policy priority but as a tool to find items that already generate a high volume of matches in general. This information allows you to consider other protective measures for these items in and outside of DLP policies. For example, you identify documents with four times as many policy matches as the next highest match count. Even though the protective action prevents these files from being shared you might consider storing them at a more secure location.

2.3.5.3. Review data loss prevention false positives and overrides

The false positives and overrides visible in this DLP report come from your users. You need to work with your users to make sure that they know how to report false positives to ensure the data in this report can be useful.

The report consolidates two different types of information, but they both help you identify the same issues with your policies. Specifically, they allow you to see instances where your users are affected by policies when they don't expect to.

For example, you created a new financial data policy in test mode, a week ago you activated policy tips and allowed overrides of the policy. If you use the reports to tune a new policy to match only when it is supposed to match you should select a start date close shortly before the time you activated policy tips and limit the scope to show you false positives.

1. In the right corner select **Filter**.
2. Select a start date.
3. Under Services, make sure all services selected.
4. Select the financial data policy you want to analyze and select Apply.
5. In the legend of the chart, uncheck **DLP policy override**.

From this view, you can observe all false positive reports of your financial data policy and use it to identify the sensitive information it falsely matched. Reviewing the matching content gives you more information about how to modify the matching policies.

Overrides can help you identify business processes that will be affected by your policy. If you get a high volume of Overrides on a policy, you should review the business process. You need to determine if you can adjust the policy without negatively affecting its protective functions. To do this follow these steps:

1. In the legend of the chart, select **DLP overrides** and uncheck **DLP false positives**.
2. Select an item on the table and review the Justification section of the pop-up.
3. Overrides are not negative. They help with auditing because it holds the user accountable for the override and allows you to review if legitimate reasons require the DLP policy override.

2.3.6. Manage permissions for data loss prevention reports

To view DLP reports in the Compliance center, you must be assigned to the:

MANAGE PERMISSIONS FOR DATA LOSS PREVENTION REPORTS

Role	Roles assigned to Role group:	Purpose
Security Reader (Exchange)	Organization Management, Security Reader	Assigning users to role groups containing this role grants them the same permissions as assigning those users to the Security & Compliance Center Security Reader role because permissions are synchronized between them.
View-Only DLP Compliance Management	Compliance Administrator, Organization Management, Security Administrator, Security Reader	This is a base role that grants read-only access to the DLP Reports in the Security & Compliance Center. Use it to create new role groups in your organization.

Members of your compliance team who read DLP policy reports need permissions to the Compliance Center. By default, your tenant admin will have access to this location and can give compliance officers and other people access to the Microsoft 365 Compliance center, without giving them all the permissions of a tenant admin. To do this, you should:

1. Create a group in Azure AD and add compliance officers to it.
2. Create a role group on the **Permissions** page of the **Compliance Center**.
3. While creating the role group, use the **Choose Roles** section to add the following role to the Role Group: **View-Only DLP Compliance Management**.
4. Use the **Choose Members** section to add the group you created before to the role group.

You can also create a role group with administrative privileges to the DLP policies and DLP reports by granting the **DLP Compliance Management** role.

Instead of creating a new role group you can also assign one of the existing role groups in the Compliance Center under Permissions. If you want users to have read-only access to the existing reports pages, you can assign the Security Reader role.

Role groups for the Compliance Center might have similar names to the role groups in Exchange Online, but they are not the same.

2.3.7. Manage and respond to data loss prevention policy violations

When a DLP policy alert informs you about a DLP policy violation, it can mean many things. Not all alerts mean that data loss is imminent or was prevented. DLP policies will not make decisions about the reason for attempting to share protected data, but they will alert you if a violation is observed. Reacting to policy violations can include escalating issues to your security team and working closely with other business stakeholders. You should know the process for contacting other teams and security before it is necessary.

For example, you protect financial information in your organization to prevent sharing of customer data with third parties but at the end of the first month you get alerts about rule violations on your financial information policy. Reviewing the reports shows a high number of e-mails from the accounting department including billing information for your customers. The policy reacted to the sensitive customer information without taking context into account. A compliance administrators' role is to assess and evaluate policy violations and act accordingly. In this instance, you should accept that the end of the month information will trigger alerts because it correctly identifies protected data and

informs you about this fact. You might want to adjust the instance count of the policy to reduce the number of alerts, but this could have negative effects on the policy at other times of the month.

Now consider that you later created a personal data policy that displays an alert spike around the same time at the end of each month as the financial information policy. Looking at the new spike in your personal data policy shows you the violation happens on the same items as the financial information policy. You decide to take a closer look at the billing documents and notice that they include personal identifiable information beyond what is immediately necessary for billing documents. In this case, you should not adjust the policies to avoid triggering at the end of the month. Instead, you should reach out to the responsible party and identify if this information is needed in the current business process and if not, why it is created in the first place.

A technical solution to this problem would be to allow the accounting department to override the block action of the personal data policy but this will increase the time they need to send out billing information because they would need to override each policy match. If you cannot work with the accounting department on reducing the amount of shared personal data you can still adjust the sensitivity, instance count, or exclusions of your policy to reduce the number of alerts at the end of each month.

DLP reports can also help you identify users who create a high number of matches. There may be multiple reasons and your role as a compliance administrator is to evaluate if the matches are benign or malevolent. For example, a user in the accounting department might generate a high number of matches at the end of each month because of the financial information policy and the monthly business process of sending out billing information. This is most likely benign, but you should take a closer look at all occurrences of a high alert count. Users who are aware of these policies, because of policy tips or because they have worked with you on creating them, might use that knowledge to share information they should not share. If a malevolent user decides to send out financial information, they could use the end of the month to hide the malevolent mails in between the legitimate mails from your business process.

You can also use the reports to allow your users to help you with refining the DLP policies. For this, you can use the DLP false reports and overrides report. If you allow users, the ability to override using a business justification they not only hold themselves accountable by choosing the override, but they also allow you to review the reason and identify business processes that warrant an adjustment to your policy or the business process itself.

For example, you open the false positives and overrides report and notice a high number of false positives on your Tax Identification Number policy. Opening the details of these false positives you see that your internal product numbers look like European tax identification numbers, which result in users reporting these matches as false positives.

2.3.7.1. Configure DLP rule exclusions

You decide to adjust the Tax identification number DLP policy to exclude instances where it matches your custom sensitive information type for Product Number. To do this, follow these steps:

1. In the M365 compliance center, on the **Policies** page, expand Data and select **Data loss prevention**.
2. Check the Tax identification number policy and select **Edit Policy**.
3. Select **Next** twice to get to the rules page and edit the rule that creates numerous false positives.
4. Expand Exceptions and select **Add Exception**.
5. From the dropdown menu, select **Except if content contains**.
6. Select **Add** and select sensitive info types.
7. From the pop-up select the custom product number info type and select **Add**.
8. Select **Save**.
9. Select **Next** twice, review the policy and select **submit**.

This will reduce the number of false positives of your policy because now it won't apply when it identifies product numbers in your users shared content.

If a malevolent user is aware of the matching indicators, they can use them to create a match on the product numbers exclusion and circumvent the protective actions of this rule by purposefully including a matching exclusion.

2.3.8. Knowledge check

Choose the best response for each of the questions below. Then select **Check your answers**.

2.3.8.1. Question 1

1. A security operations analyst wants to fine-tune their DLP policies before activating policy tips. Which report should they use to gather information?

- DLP incidents
- DLP policy matches
- DLP false positives and overrides

2.3.8.1.1. Correct Answer

- DLP policy matches

This is correct. This report shows you all rule matches and allows you to review the accuracy of matches for fine-tuning.

2.3.8.1.2. Wrong Answer

- DLP incidents

This is not correct. This report is used to identify items with a high volume of matches.

- DLP false positives and overrides

This is not correct. This report allows you to fine-tune policies based on user input.

2.3.8.2. Question 2

2. A security operations analyst wants to fine-tune their DLP policies based on user input. Which report should they use to gather information?

- DLP false positives and overrides
- DLP incidents
- DLP policy matches

2.3.8.2.1. Correct Answer

- DLP false positives and overrides

This is correct. You can allow users to report false positives and override protective actions. You can use the information of these actions to reduce the number of false positives or interruptions of legitimate business processes.

2.3.8.2.2. Wrong Answer

- DLP incidents

This is not correct. This report is used to identify items with a high volume of matches.

- DLP policy matches

This is not correct. This report shows you all rule matches and allows you to review the accuracy of matches for fine-tuning but it is not based on user input.

2.3.8.3. Question 3

3. A security operations analyst wants to identify items in their organization that might contain a high volume of sensitive information based on your DLP policies. Which report should they use to gather information?

- DLP false reports and overrides
- DLP incidents
- DLP policy matches

2.3.8.3.1. Correct Answer

- DLP incidents

This is correct. This report is used to identify items with a high volume of matches which can indicate a high volume of sensitive information.

2.3.8.3.2. Wrong Answer

- DLP false reports and overrides

This is not correct. This report shows you all rule matches and allows you to review the accuracy of matches for fine-tuning but it is not based on user input.

- DLP policy matches

This is not correct. This report shows you all rule matches and allows you to review the accuracy of matches for fine-tuning and to identify business processes

2.3.8.4. Question 4

4. Which default role can you assign if you want to grant someone read-only permissions on DLP reports without allowing them to make changes?

- Security Reader
- Security Administrator
- Compliance Administrator

2.3.8.4.1. Correct Answer

This is correct. The role only grants read-only permission to Compliance reports.

2.3.8.4.2. Wrong Answer

- Security Administrator

This is not correct. Security Administrator allows ability to read and manage security configuration and reports.

- Compliance Administrator

This is not correct. This role has full access to the Compliance Center and can make changes.

3. Implement Information Governance in Microsoft 365

3.1.Govern information in Microsoft 365

3.1.1. Information governance overview

Information governance helps you manage the end-to-end lifecycle of all content across your organization's digital estate, including Microsoft 365, third-party clouds, hybrid deployments, and any content you bring into Microsoft 365. Trainable classification and automated retention simplify the governance process. It is about keeping the data necessary for business, regulatory, legal, or other reasons, and removing any data from

your digital estate that should not be kept. This decreases your attack surface and minimizes compliance risk.

Retention policies help ensure you retain content as long as it is required, but no longer. With information governance, you can take two approaches to retention. You can use organization-wide policies, and you can use label-driven policies applied manually by a user or automatically by Microsoft 365.

Using organization-wide policies, you can choose to retain content for a specific time period or permanently delete content at the end of the retention period. Policies can apply to one or more locations where information is stored like Exchange Online, SharePoint Online and Microsoft Teams.

Label-driven policies enable users to contribute to the accuracy of your data retention implementation. Users can manually label their own content to classify it. You can also auto-apply labels to specific content to make things easier on users. As with organization-wide policies, you can choose to retain or delete content based on when it was created or last modified. In addition, you can base retention on when it was labeled or an event, such as an employee leaving the organization. Retention labels can be automatically applied to content containing sensitive data, specific words or phrases, or having certain metadata, or that it matches a trainable classifier.

3.1.1.1. Customer scenarios

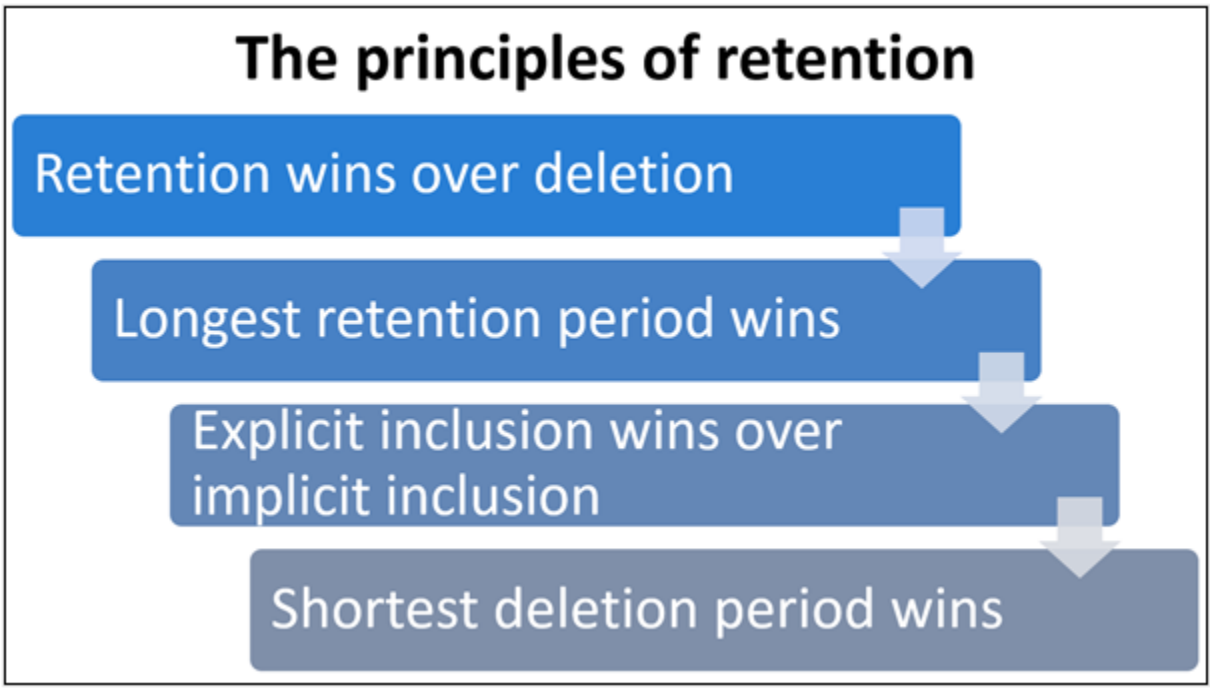
Here is some common scenarios Microsoft's solution for information governance can address:

- Create an organization-wide retention policy to delete all Microsoft Teams communications older than seven days.
- Review documents stored in a SharePoint document library prior to them being deleted because a retention policy expired.
- Implement a 5-year retention policy where automatically labeled content will be kept five years and then automatically deleted.

3.1.1.2. Retention policy precedence

Situations may arise where content has several retention policies apply (or a combination of retention policies and a single retention label policy). These policies might have different actions (retain, delete, or both) and different retention periods. The following retention principles explain what takes precedence. The principles are applied

from top to bottom. If the rules applied by all policies are the same at one level, the flow moves down to the next level to determine which rule is applied.



3.1.1.2.1. Retention wins over deletion

Suppose one retention policy says to delete Exchange email after three years, but another retention policy says to retain Exchange email for five years and then delete it. Any content that reaches three years old will be deleted and hidden from the user, but still retained in the Recoverable Items folder until the content reaches the five-year retention period. Then it would be permanently deleted. Content being retained by one policy cannot be permanently deleted by another policy.

3.1.1.2.2. Longest retention period wins

If content is subject to multiple policies that retain content, it will be retained until the end of the longest retention period.

3.1.1.2.3. Explicit inclusion wins over implicit inclusion

If a label with retention settings is manually assigned (known as an explicit label) by a user to an item, such as an Exchange email or OneDrive document, that label takes precedence over a policy assigned at the site or mailbox level or a default label assigned by the document library. For example, if the explicit label says to retain the item for 10 years, but the policy assigned to the site says to retain it for five years, the label takes

precedence. Auto-applied labels are considered implicit, not explicit, because they are applied automatically by Microsoft 365.

If a retention policy includes a specific location, such as a specific user's mailbox or OneDrive account, that policy takes precedence over another retention policy that applies to all users' mailboxes or OneDrive accounts but does not specifically include that user's mailbox.

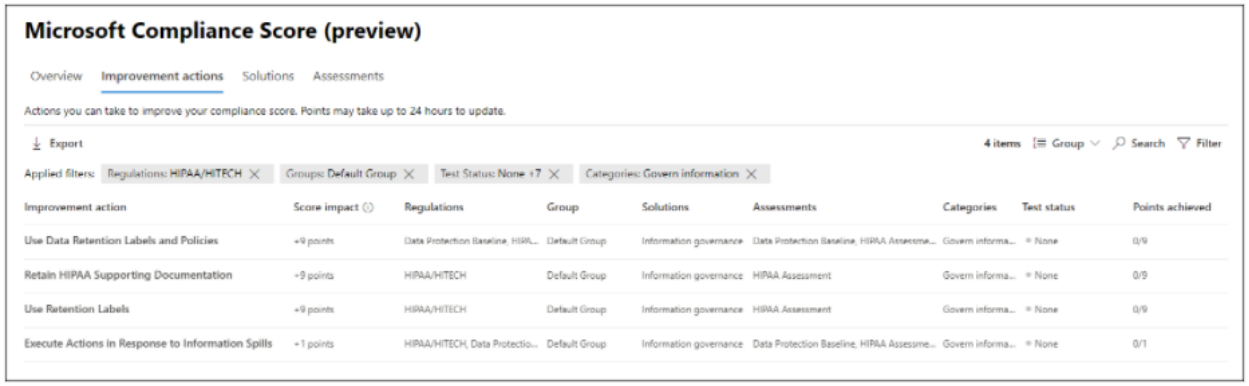
3.1.1.2.4. Shortest deletion period win

If content is subject to multiple policies that delete content (with no retention), it will be deleted at the end of the shortest retention period.

3.1.1.3. Getting started with information governance

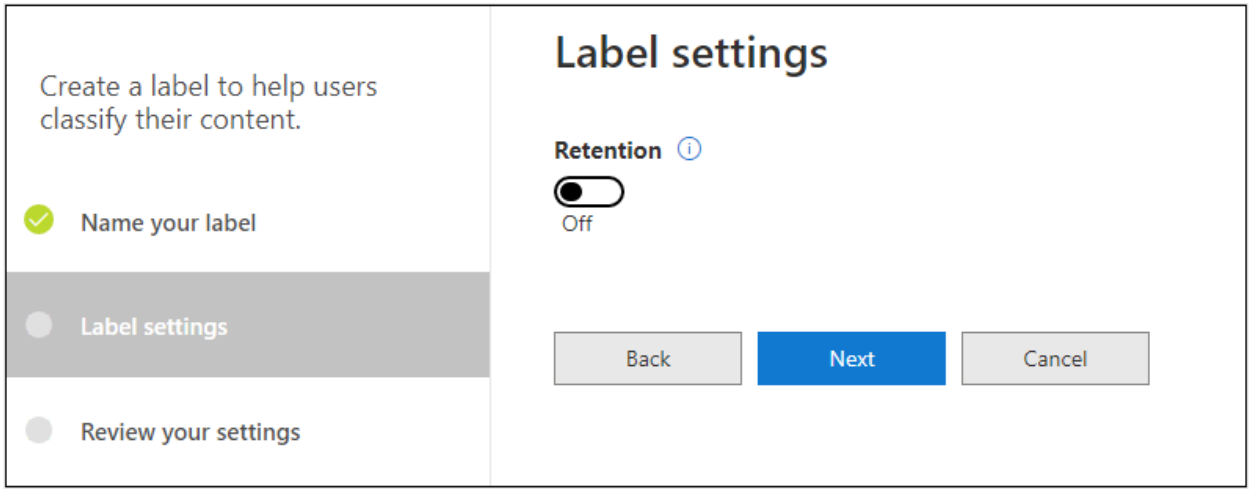
Deciding what you want to keep and for how long is at the core of information governance. Business, legal, and compliance requirements can impact your information governance strategy. Those responsible for information governance in your organization should identify the content to retain or dispose for business and legal requirements. The governance team will also need to identify the regulations that apply to your organization, many of which include information governance requirements.

Microsoft Compliance Score maps these compliance regulations, like the US Health Insurance Portability and Accountability Act (HIPAA), to actions recommended to achieve compliance. Many of these actions can be addressed using the **Information governance** solution. The image below shows the improvement actions in the **Information governance** solution the organization can take to improve its compliance posture relative to HIPAA.



One of the first steps in creating a retention label is to tell Microsoft 365 if you want to apply retention settings. You may want to consider keeping this setting **Off** when

creating and publishing (or auto-applying) a new label. You can then modify the retention label settings to add a retention period once you are satisfied it is working correctly. The image below shows the step during the retention label creation process where you specify if you want the label to apply retention. It may take as long as seven days for new retention labels to take effect after you publish or auto-apply them, so plan accordingly.



The instructions in the rest of this module assume you have added **Information governance** to the **Microsoft 365 compliance center** menu. This is also recommended if you are going to be working with the solution frequently. Here are the steps:

1. Open **Microsoft 365 compliance center** in your web browser address bar.
2. Click **Customize navigation**.
3. Check the box that says **Information governance**.
4. Click **Save**.

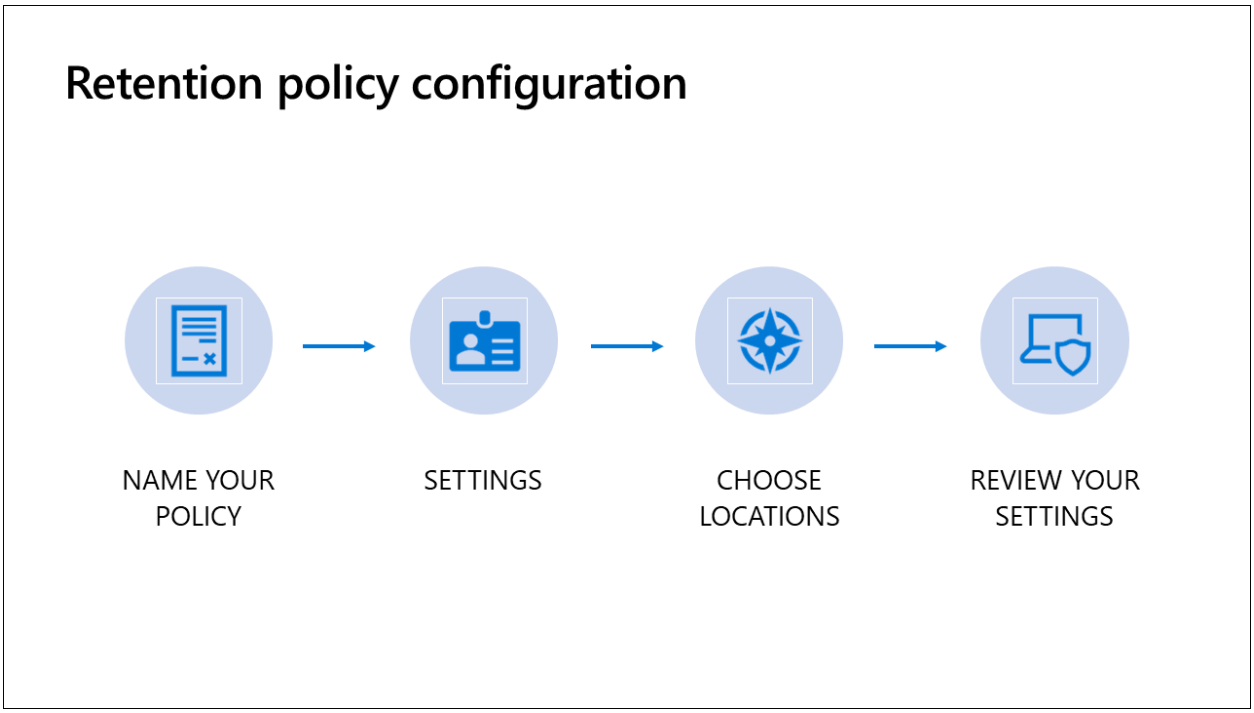
3.1.2. Configure retention policies

Email, documents, Skype for Business, and Teams conversations. Your users generate a lot of content every day. Take control of it by setting up retention policies to keep what you want and get rid of what you don't. Users can continue to edit and work with the content when it is subject to a retention policy, because the content is retained in place, in its original location. If someone edits or deletes content subject to the policy, a copy is saved to a secure location where it is retained while the policy is in effect.

Navigate to **Microsoft 365 compliance center > Information Governance > Retention to configure retention policies**.

Creating a retention policy consists of these steps.

1. Name your policy
2. Settings
3. Choose locations
4. Review your settings



3.1.2.1. Step 1: Name your policy

3.1.2.1.1. Name

Enter a short name for the retention policy to be displayed on the Retention page.

3.1.2.1.2. Description

Enter a description of the retention policy's purpose.

3.1.2.2. Step 2: Settings

The first decision you need to make when configuring the settings for the retention policy is which path to take: basic or advanced. The basic path, along with its branches, is represented by the settings under the heading, **Do you want to retain content?** The advanced path is represented by the settings under the heading. **Need more options?** The basic branch applies to all content in the locations you choose, while the advanced path lets you set more granular application options.

While the advanced **Need more options?** path still exists today, a best practice is to use retention labels instead when you need to apply granular retention settings. It is not covered here for that reason.

3.1.2.3. Do you want to retain content?

You will have to provide additional information based on if the answer to this question is yes or no.

3.1.2.3.1. Yes, I want to retain it.

Selecting this option means the content will stay where it is for the time period specified. For example, email and Teams conversations will stay in mailboxes and documents will stay in SharePoint or OneDrive. If users delete the content, a copy will be placed in a secure location so you can access it, if needed.

In addition to specifying the amount of time to retain the content before it is disposed, you must specify when you want the retention period timer to start. The options are **when it was created** and **when it was last modified**. The settings here behave differently for content in different locations.

3.1.2.4. SharePoint and OneDrive documents:

3.1.2.4.1. When it was created.

The retention period begins when documents were created.

3.1.2.4.2. When it was last modified.

The retention period begins based on when documents were last modified.

3.1.2.5. Email messages and Teams conversations:

3.1.2.5.1. When it was created or when it was last modified.

Regardless of what you choose, the retention period on content in email messages and Teams conversations will be based on when messages or conversations were sent or received.

Next, select if you want to delete the content after the retention period has expired. Options are **Yes** and **No**. There is no option for the content to go through a disposition review.

- **Yes**. After this time, content is deleted from where it is stored and from the secure location where copies are kept.
- **No**. Content will be left in place. If you do not want to keep the content, you must delete it yourself.

No, just delete content older than. Users will be free to permanently delete their content any time prior to expiration. When the content reaches the age selected, it will be deleted without the user having to do anything. For example, email messages and calendar items will be deleted from users' mailboxes and documents will be deleted from their SharePoint or OneDrive libraries.

In addition to specifying the amount of time that must pass before content is deleted you must determine when you want the timer to start. The options are **when it was created** and **when it was last modified**. The settings behave differently for content in certain locations.

SharePoint and OneDrive documents:

- **When it was created**. Documents will be deleted based on when they were created.
- **When it was last modified**. Documents will be deleted based on when they were last modified.

Email messages and Teams conversations:

- **When it was created or when it was last modified**. Regardless of what you choose, the retention period on content in email messages and Teams conversations will be based on when messages or conversations were sent or received.

Step 3: Choose locations

The first option is **Apply policy only to content in Exchange email, public folders, Microsoft 365 groups, OneDrive, and SharePoint documents**. No additional options are provided if you select this option.

The second option offers you more control. In addition to selecting more locations, you can also include or exclude locations based on additional parameters. For example, you can include only the Finance department's SharePoint site in the retention policy. The

following table shows the options and the additional control to refine the retention policy scope.