

Five data modeling tips for better data governance + Data Classification

bron:

 Idera-wp-5-data-modeling-tips-for-bett... 2 MB

Geanoteerd

 Idera-wp-5-data-modeling-tips-for-bett... 2 MB

Dit artikel beoogd om datamodellen te verreiken met meta afkomstig van Data Stewards tav classificatie/beveiliging en definities

Toont ook de mogelijkheid om

data classificatie door Microsoft SQL server management server te doen (geldt voor SSMS versie >=17.5 (en SSMS Versie >=18.4 met een SQL2019 database in docker image)

<https://www.youtube.com/watch?v=Kq0oihK4wIA> (video) zie 11:08.

<https://docs.microsoft.com/en-us/sql/relational-databases/security/sql-data-discovery-and-classification?view=sql-server-ver15&tabs=t-sql> (doc)

en/of handmatig obv t-sql op de database

https://docs.microsoft.com/en-us/sql/t-sql/statements/add-sensitivity-classification-transact-sql?view=sql-server-ver15&WT.mc_id=DP-MVP-5001259

zie ook [Howto data classificeren van Database kolommen in een SQL2019 database mbv t-sql](#) (files nog export naar git)

zie ook [How To Opvragen van de data geclassificeerde Database kolommen in een SQL database](#) (files nog export naar git)

en/of data classificatie gedaan door **Microsoft Data Discovery & Classification built-in van Azure databases** (azure managed instance, azure sql database, azure synapse analytics).

<https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview>

Microsoft Information Protection Policy (MIP)

zie <https://docs.microsoft.com/en-us/sql/relational-databases/security/sql-data-discovery-and-classification?view=sql-server-ver15&tabs=t-sql#classify-your-database-using-microsoft-information->

Voorbeeld van een export van een MIP uit SSMS 18.11.1 in json format:

 Information_Protection_Policy_export... 61 kB

De Microsoft sensitivity labels en de MIP worden gemaakt mbv Microsoft Purview (voorheen Microsoft 365 compliance)

zie <https://docs.microsoft.com/en-us/microsoft-365/compliance/create-sensitivity-labels?view=o365-worldwide>

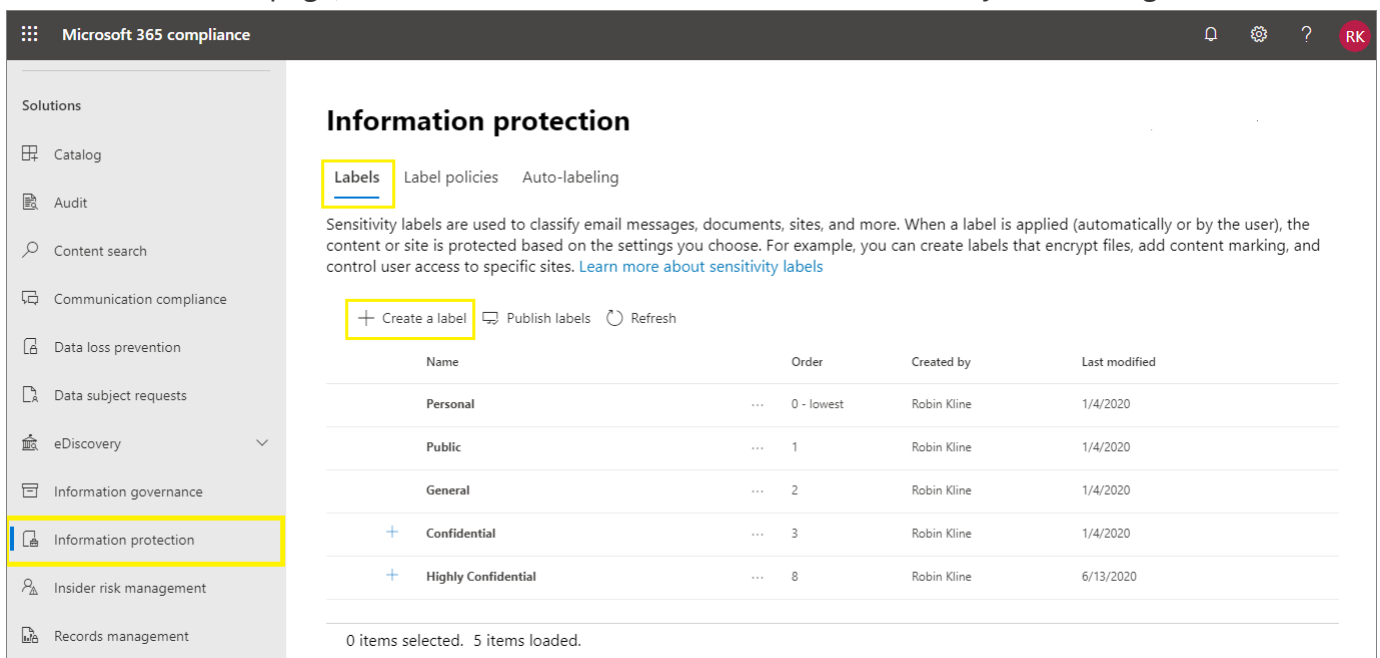
All Microsoft Purview Information Protection solutions are implemented by using sensitivity labels. To create and publish these labels, go to the Microsoft Purview compliance portal.

De labels kunnen dan gebruikt worden om data te beschermen obv labels in MS Office, Share Point, Microsoft on-premise SQL server en Azure SQL databases en in apps.

Create and configure sensitivity labels

1. From the Microsoft Purview porta, select Solutions > Information protection
If you don't immediately see this option, first select Show all.

2. On the Labels page, select + Create a label to start the New sensitivity label configuration:



Information protection

Labels Label policies Auto-labeling

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. [Learn more about sensitivity labels](#)

+ Create a label Publish labels Refresh

Name	Order	Created by	Last modified
Personal	0 - lowest	Robin Kline	1/4/2020
Public	1	Robin Kline	1/4/2020
General	2	Robin Kline	1/4/2020
+ Confidential	3	Robin Kline	1/4/2020
+ Highly Confidential	8	Robin Kline	6/13/2020

0 items selected. 5 items loaded.

Create a sensitivity label.

Note

By default, tenants don't have any labels and you must create them. The labels in the example picture show default labels that were migrated from Azure Information Protection.

3. On the Define the scope for this label page, the options selected determine the label's scope for the settings that you can configure and where they will be visible when they are published:

Define the scope for this label

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

☒ **Files & emails**

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

☒ **Groups & sites**

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

☒ **Schematized data assets**

Apply labels to files and schematized data assets in Azure Purview. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

Scopes for sensitivity labels.

- If Files & emails is selected, you can configure settings that apply to apps that support sensitivity labels, such as Office Word and Outlook. If this option isn't selected, you see the first page of these settings but you can't configure them and the labels won't be available for users to select in these apps.
- If Groups & sites is selected, you can configure settings that apply to Microsoft 365 groups, and sites for Teams and SharePoint. If this option isn't selected, you see the first page of these settings but you can't configure them and the labels won't be available for users to select for groups and site.

For information about the Schematized data assets scope, see [Automatically label your content in Microsoft Purview Data Map](#).

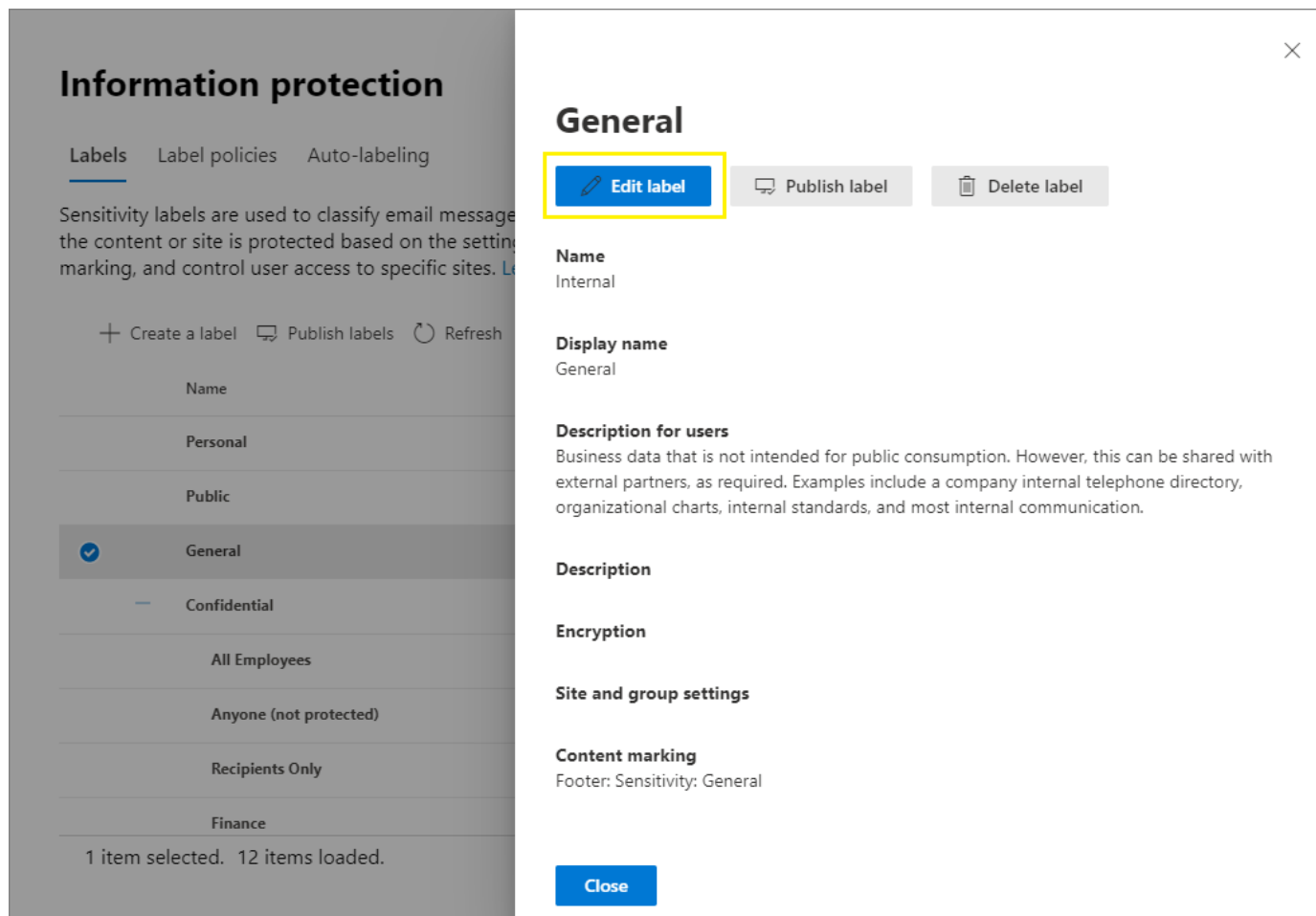
4. Follow the configuration prompts for the label settings.

For more information about the label settings, see [What sensitivity labels can do](#) from the overview information and use the help in the UI for individual settings.

5. Repeat these steps to create more labels. However, if you want to create a sublabel, first select the parent label and select ... for More actions, and then select Add sub label.

- When you have created all the labels you need, review their order and if necessary, move them up or down. To change the order of a label, select ... for More actions, and then select Move up or Move down. For more information, see Label priority (order matters) from the overview information.

To edit an existing label, select it, and then select the Edit label button:



Edit label button to edit a sensitivity label.

This button starts the Edit sensitivity label configuration, which lets you change all the label settings in step 4.

Don't delete a label unless you understand the impact for users. For more information, see the Removing and deleting labels section.

Publiceren

Om sensitivity labels te kunnen gebruiken moeten ze gepubliceerd worden vanuit Microsoft Purview

Voorbeeld scripts

Voorbeeld script om bv json file sensitivity labels aan te maken met informatie typen.

Deze json file wordt dan ingelezen in Microsoft SQL server Management Server voor een bepaalde database,

waarna deze definities gebruikt kan worden om de kolommen in de tabellen van de database te kunnen

Data Classificeren.

 vb_scripts_auto_Data_Classificatie_mb... 2 MB