

Upload Custom Sensitive Information Types in Office 365



Vlad Catrinescu

OFFICE SERVERS AND SERVICES MVP

@vladcatrinescu <https://absolute-sharepoint.com>



Overview



How is this useful?

The PowerShell script to do it



How Is This Useful?





Your business can store sensitive information types

Employee IDs

Patient numbers

Social Security numbers

Credit Card numbers

Office 365 has built-in Data Loss Prevention (DLP) policies

Office 365 allows you to create your own rules





Custom Sensitive Information Types are created in an XML file

You can specify

- Pattern (Regex)
- Keywords
- Proximity information
- Different confidence levels based on information found



Custom Sensitive Information Types cannot be uploaded via the Office 365 Admin Center

You need to upload them by using PowerShell





We will not cover how to create the XML file

- DLP in Office 365 is part of a bigger, compliance focused topic

We will focus on managing the policies with PowerShell

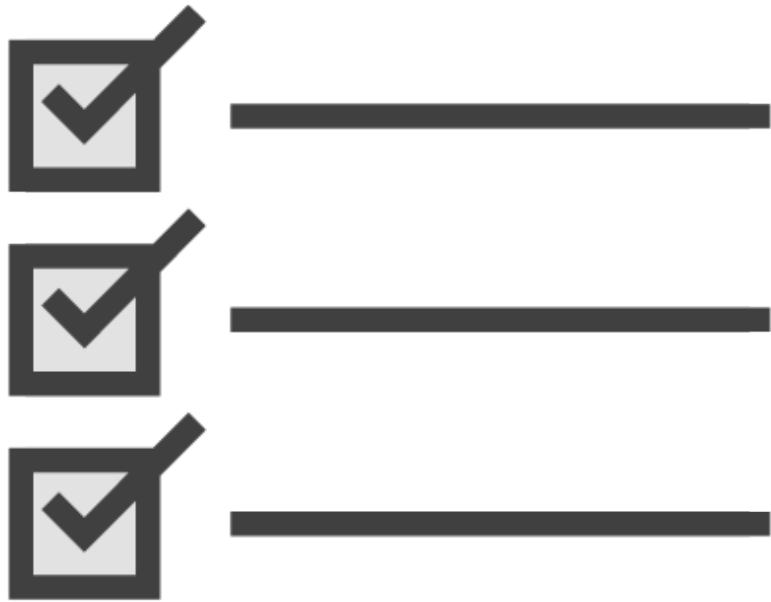
Microsoft Resources:

- <https://support.office.com/en-us/article/create-a-custom-sensitive-information-type-82c382a5-b6db-44fd-995d-b333b3c7fc30>
- <https://support.office.com/en-us/article/customize-a-built-in-sensitive-information-type-2164ce3d-4d64-4283-b6b1-b81fbe835e8e>
- <https://docs.microsoft.com/en-us/office365/enterprise/customize-or-create-a-new-sensitive-information-type>



Upload Custom Sensitive Information Types in Office 365 with PowerShell





**The Office 365 Compliance Center
PowerShell Module**

**Organizational Management role in the
Office 365 Compliance Center**

The XML Rule Pack you want to upload

Sample used for this course included in
course downloads



New-DlpSensitiveInformationTypeRulePackage

Use the New-DlpSensitiveInformationTypeConfig cmdlet to import data loss prevention (DLP) sensitive information type rule packages in the Security & Compliance Center



Upload a Sensitive Information Type

```
New-DlpSensitiveInformationTypeRulePackage  
  -FileData (Get-Content -Path  
"C:\Pluralsight\EmployeeIDRulePack.xml" -Encoding Byte)
```



Export an XML File of the Current Rules

```
$ExistingRules = Get-DlpSensitiveInformationTypeRulePackage
```

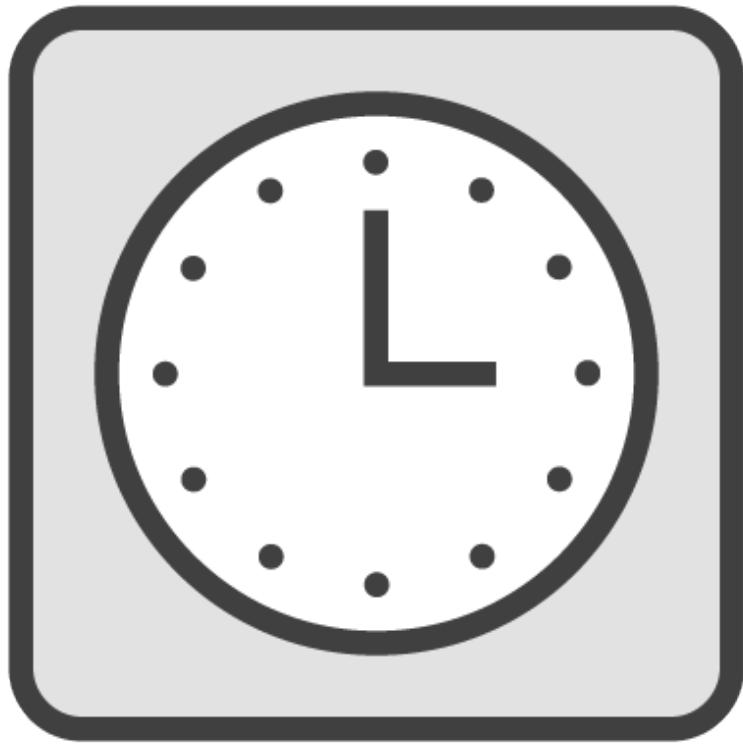
```
Set-Content
```

```
-Path "C:\Pluralsight\exportedRules.xml"
```

```
-Encoding Byte
```

```
-Value $ExistingRules.SerializedClassificationRuleCollection
```





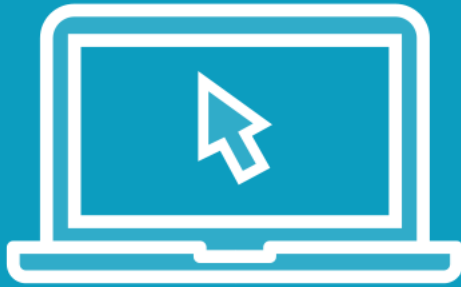
DLP uses the search crawler to identify and classify sensitive information in SharePoint and OneDrive for Business

You can manually request a re-index on a site, list or library

If you uploaded multiple rules that apply to all SharePoint content, contact Office 365 Support and request a full tenant crawl



Demo



Upload Custom Sensitive Information Types in Office 365 with PowerShell



Conclusion



Your business can store sensitive information types

Office 365 has built-in Data Loss Prevention (DLP) policies

Office 365 allows you to create your own rules

XML file format

Rules can only be uploaded via PowerShell

New-
DlpSensitiveInformationTypeRulePackage

