

# Adding Classifications to Office 365 Groups

---



**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?

---





**Users will be able to select a classification for Office 365 groups**

**Classifications do not technically change anything in the Office 365 group**

**They are shown at the top of every group / SharePoint site/ team , etc.**

Helps with user awareness of data sensitivity

**Classifications are visible via PowerShell**

You can use PowerShell to create different reports based on classification for example



# Create a group

A group provides a space for shared conversations, files, a group calendar

Group name

Description

Tell people t

Privacy

Public - Any

Classification

Confidential

Restricted

Confident

Secret

Top Sece

## Create your team

Collaborate closely with a group of people inside your organization based on project, initiative, or common interest. [Here's a helpful video](#)

Team name

Project XTZ

GRP Sales Project XTZ United States ⓘ

Description

Privacy

Private - Only team owners can add members

Classification

Restricted

isting Office 365 group?  
group. You can add Microsoft Teams functionality without changing  
Microsoft Teams functionality

Cancel Next

Stream group connected to an Office 365 group as an easy way to organize who has permission  
ur videos and channels.

Group email alias

group\_email\_alias @...

Make this group companywide ⓘ

Allow members to contribute ⓘ

Owner ⓘ

Cancel Create

?

😊

👤

company.

on't show this again



In order to use this feature all users inside Office 365 Groups need to have an Azure Active Directory Premium license

**Licenses are not enforced by PowerShell**

It will allow you to configure it even if you don't have the license requirements  
Microsoft will send a report of users who do not comply every month





Licensing changes often in Office 365, for any licensing questions talk to your Microsoft Licensing partner

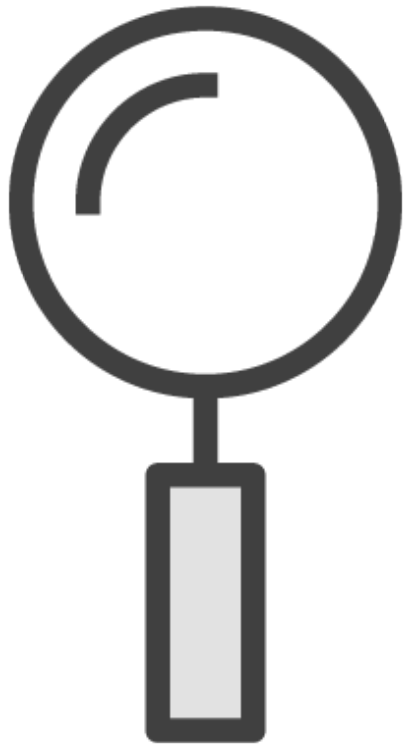


# Adding Classifications to Your Office 365 Groups

---







**Identify the classifications that are appropriate to your business**

- Restricted
- Confidential
- Secret
- Top Secret

**You can specify a default classification**

**You can add a description for each classification to explain to users what each level is for**



## AzureAD PowerShell module

- Preview module used at the time of recording this course
- Cmdlets will make it in the production module

**We will create/modify an Active Directory settings object inside Azure Active Directory**



Another admin might have already created a setting object for Office 365 Groups

Make sure you check if there is an existing one before creating a new one



# Viewing the Values of an Existing Active Directory Setting Object

```
$Setting = Get-AzureADDirectorySetting | `
    where-object {$_.displayname -eq 'Group.Unified'}
$Setting.Values
```



# Creating a New Active Directory Setting Object

```
$SettingTemplate = Get-AzureADDirectorySettingTemplate |  
where {$_.DisplayName -eq 'Group.Unified' }
```

```
$NewAADSetting = $SettingTemplate.CreateDirectorySetting()
```

```
$NewAADSetting = New-AzureADDirectorySetting `   
-DirectorySetting $NewAADSetting
```



# Configuring the Setting

```
$Setting = Get-AzureADDirectorySetting | `
    where-object {$_.displayname -eq 'Group.Unified'}

$Setting["ClassificationList"] =
    "Restricted, Confidential, Secret, Top Secret"

$Setting["DefaultClassification"] = "Confidential"
```



# Classification Description

```
$Setting["ClassificationDescriptions"]="Restricted:Restricted material would cause undesirable effects if publicly available,Confidential:Confidential material would cause damage or be prejudicial to national security if publicly available,Secret:Secret material would cause serious damage to national security if it were publicly available,Top Secret:Top Secret is the highest level of classified information"
```

```
Set-AzureADDirectorySetting -Id $Setting.id `
    -DirectorySetting $Setting
```

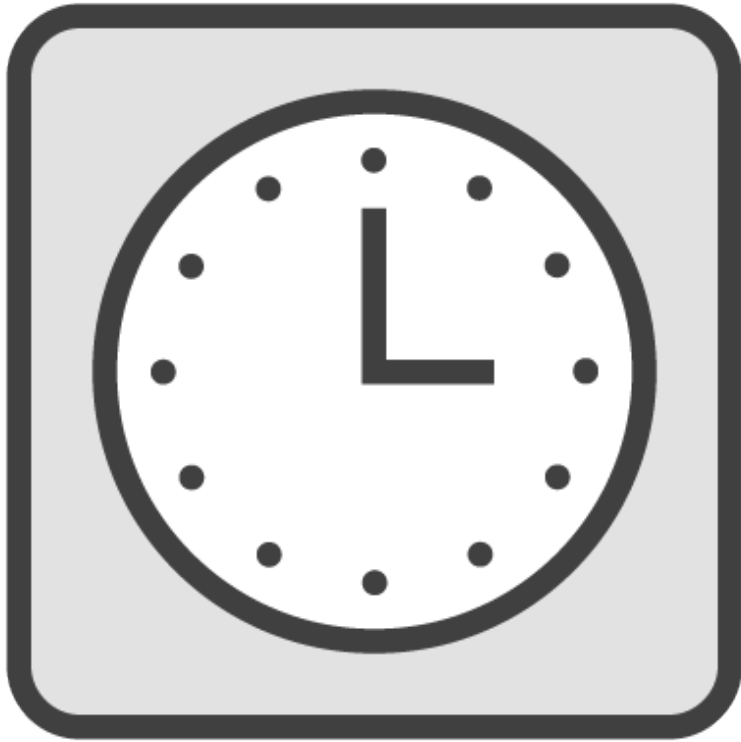


# Setting a Classification by PowerShell

```
Set-UnifiedGroup `
  -Identity "2019reorg" `
  -Classification "Top Secret"
```





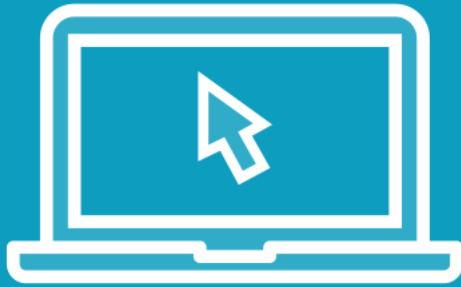


**It might take a while for the configuration to be reflected in the user interface**

- Some Office 365 applications apply it faster than others



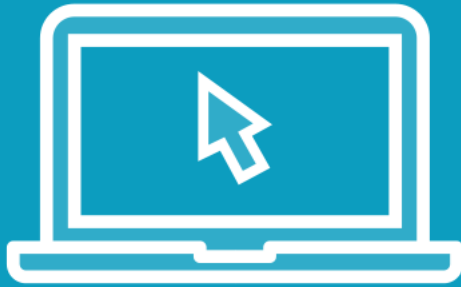
# Demo



## Setting classifications in Office 365 Groups



# Demo



## User experience in Office 365



# Conclusion



Different content can have different security, and compliance requirements

Classifications do not change anything technically

A classification is visible across services in that group, raising awareness

Classifications can be queried by PowerShell, allowing you to automate tasks, or reports

