

# How to protect my data in Office 365?

Dutch Microsoft & Security Meetup – 23 mei 2019



# Maarten Eekels



## Portiva.

Microsoft  
Regional Director



### Contact

 @maarteneekels  
meekels@portiva.nl  
[www.eekels.net](http://www.eekels.net)

Em



Office 365

Office 365 c

"Quarantine

You can rev

Review

Sincerely,  
The Microsc

Microsoft Corp

This message v

[Privacy](#) | [Legal](#)

Organization: portiva Email Exchange

Hello [meekels@portiva.nl](mailto:meekels@portiva.nl),

To continue sending messages, please [sign in meekels@portiva.nl](#)

This helps us stop automated programs from sending junk email.

Thanks for your help and patience!

[Sign in to meekels@portiva.nl Office 365 Account](#) if you c

[View this message in the Office 365 message center](#)

To customize what's included in this email, who gets it, or

If you are receiving this email because your Admin added  
unsubscribe.

[Edit release preferences](#)

Choose the release track for your organization. Use these

*Microsoft respects your privacy. To learn more, please read c*

Microsoft Corporation  
One Microsoft Way  
Redmond, WA, USA 98052

[Unsubscribe](#)

Hello [meekels@portiva.nl](mailto:meekels@portiva.nl),

Microsoft Outlook cannot synchronize your INBOX folder, due to account validation error, so the IMAP server cannot fetch new incoming messages , click on the "fix imap error" button to fix this issue.

Thanks for subscribing to Office 365. We hope to continue serving you.

## FIX IMAP ERROR

### Subscription information:

Organization: portiva Corporation

Subscription ID: bf9c78dd-f268-47c5-b710-b1488ff996a1

### Helpful resources

[Get help and support for meekels@portiva.nl](#)

This is a mandatory service communication. To set your contact preferences for other communications, visit the [Promotional Communications Manager](#).

This message was sent from an unmonitored e-mail address. Please do not reply to this message.

[Privacy](#) | [Legal](#)

Microsoft Office  
One Microsoft Way  
Redmond, WA  
98052-6399 USA



# Agenda

- Data encryption
- Multi-factor authentication
- Azure AD identity protection
- Conditional access
- Azure AD privileged identity management
- Office 365 unified labelling
- Data loss prevention

# Data encryption

## Data at rest

- BitLocker drive encryption
- Per-file encryption (for SharePoint Online and OneDrive for Business)
- Files are spread across multiple Azure Storage containers
- Map with file locations is also encrypted
- Encryptions keys are physically located somewhere else

## Data in transit

- TLS across all workloads
- TLS 1.2 support
- SSL 3.0 / TLS 1.0 and 1.1 support already withdrawn
- 3DES support withdrawn per July 10, 2019

# Multi-factor authentication



## Why MFA?

Because you will stop 99% of all phishing attacks!

## Azure AD vs Office 365

- Fraud alert
- Custom greetings
- Trusted IPs
- Hardware tokens



# DEMO



# Azure AD identity protection

Detect vulnerabilities and risky accounts

 Confirm sign-in compromised  Confirm sign-in safe  Risky users report

[Basic info](#) [Device info](#) [Risk info](#) [MFA info](#) [Conditional Access](#)

RISK EVENT		RISK EVENT STATE		TIME DETECTED
^ Anonymous IP address ⓘ		At risk		4/24/2019, 10:23 PM
IP address	199.249.230.73	Risk event level		Medium
Location	Dallas, Texas, US	Risk event detail		-
^ Atypical travel ⓘ		At risk		4/24/2019, 10:30 PM
First login time 4/24/2019, 9:51 PM		Second login time 4/24/2019, 10:23 PM		Travel duration 32:35
First login IP address 77.173.205.95		Second login IP address 199.249.230.73		Risk event level Medium
First login location Almere Haven, Flevoland, NL		Second login location Dallas, Texas, US		Risk event detail -
First login client		Second login client Firefox 60.0		



# DEMO



# Conditional access

## Implement automated access control decisions

### Access concerns:

- Sign-in risk
- Network location
- Device management
- Client application

### Cloud apps or actions

Select what this policy applies to

Cloud apps

User actions

Select the action this policy will apply to

☐ Register security information (preview)

Home > Conditional Access - Policies > What if

### What if

Policies

Info

Test the impact of conditional access on a user when signing in under certain conditions.  
[Learn more](#)

User

0 users selected

Cloud apps or actions

Any cloud app

IP address

Country

Device platform

Client apps (preview)

Device state (preview)

Sign-in risk

What if

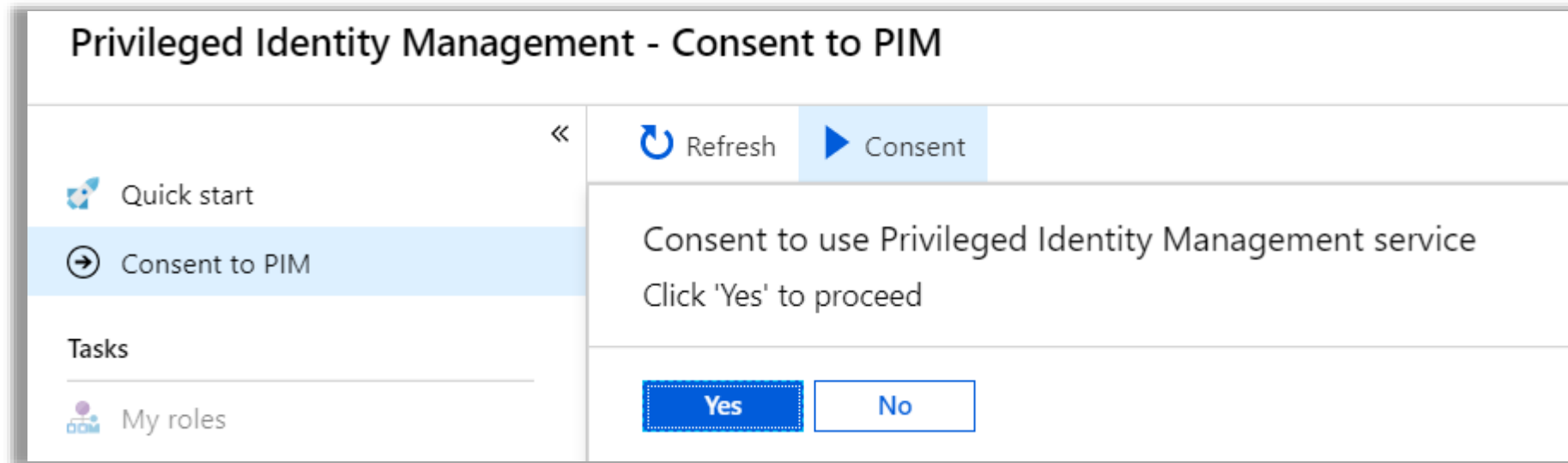
Reset

# DEMO



# Azure AD privileged identity management

Minimize the number of people who have access to secure information or resources



## Manage:

- Azure AD roles
- Azure resources

# DEMO



# Office 365 unified labelling

The screenshot displays the 'Azure Information Protection - Labels' interface. On the left, a navigation pane lists various features: General, Analytics, Classifications, Labels (highlighted with a red arrow), Policies, Scanner, and Manage. The main area shows a list of labels under the heading 'LABEL DISPLAY NAME'. The labels are: Personal, Public, Internal, Confidential, Secret, All Company, Legal, and Protection templates. A red arrow points to the 'Unified labeling' option in the 'Manage' section of the navigation pane.

**Azure Information Protection - Labels**

Search (Ctrl+/)

Columns

**General**

- Quick start

**Analytics**

- Usage report (Preview)
- Activity logs (Preview)
- Data discovery (Preview)
- Recommendations (Preview)

**Classifications**

- Labels
- Policies

**Scanner**

- Nodes
- Profiles (Preview)

**Manage**

- Configure analytics (Preview)
- Languages
- Protection activation
- Unified labeling

**LABEL DISPLAY NAME**

- Personal
- Public
- Internal
- Confidential
- Secret
- All Company
- Legal
- Protection templates

[+ Add a new label](#)

**Sensitivity** **Retention**

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](#) Search

<input type="checkbox"/>	Display name	Created by	Last modified	
<input type="checkbox"/>	Personal	Maarten Eekels	06/11/2018 13:16	...
<input type="checkbox"/>	Public	Maarten Eekels	18/12/2018 14:42	...
<input type="checkbox"/>	Internal	Maarten Eekels	14/03/2019 09:35	...
<input type="checkbox"/>	Confidential	Maarten Eekels	13/03/2019 22:45	...
<input type="checkbox"/>	Secret	Maarten Eekels	13/03/2019 23:03	...
<input type="checkbox"/>	All Company	Maarten Eekels	06/11/2018 13:17	...
<input type="checkbox"/>	Legal	Maarten Eekels	06/11/2018 13:17	...

# Unified labelling pros vs cons

## Pros

- Custom sensitive information types
- Keyword dictionaries
- Complex conditions
- Mobile client and Mac support

## Cons

- No custom permissions in Office apps
- No track and revoke
- No Do Not Forward button in Outlook

# DEMO





# Data loss prevention

## Goals of DLP:

- Identify sensitive information across Office 365
- Prevent the accidental sharing of sensitive information

## DLP policies contain:

- Locations
- Conditions
- Actions

The screenshot displays the 'New DLP policy' wizard in Microsoft 365. The left sidebar shows the progress of the four steps: 'Choose the information to protect', 'Name your policy', 'Choose locations', and 'Policy settings', all of which are completed. The 'Review your settings' step is currently active. The main content area shows the following settings:

- Template name:** Custom policy (with an 'Edit' link)
- Policy name:** Dutch Microsoft & Security Meetup (with an 'Edit' link)
- Description:** (with an 'Edit' link)
- Applies to content in these locations:** Exchange email, SharePoint sites, OneDrive accounts, Teams chat and channel messages (with an 'Edit' link)
- Policy settings:** If the content contains these types of sensitive info: EU Driver's License Number then notify people with a policy tip and email message. If there are at least 2 instances of the same type of sensitive info, block access to the content and send an incident report with a high severity level but allow people to override if they provide a business justification. (with an 'Edit' link)
- Turn policy on after it's created?** Yes (with an 'Edit' link)

At the bottom of the wizard, there are three buttons: 'Back', 'Create' (highlighted in blue), and 'Cancel'.

# DEMO



# Announcements at SPC

- Sensitivity labels for SharePoint sites
- Sensitivity label integration support
- External access expiration
- DLP restricted access (block external sharing until DLP scan has been completed)

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Updates-to-SharePoint-security-administration-and-migration/ba-p/549585>



***That's all folks!***

@maarteneekels