

Konfigurationsempfehlung zur datenschutzfreundlichen Tenantkonfiguration

Inhalt

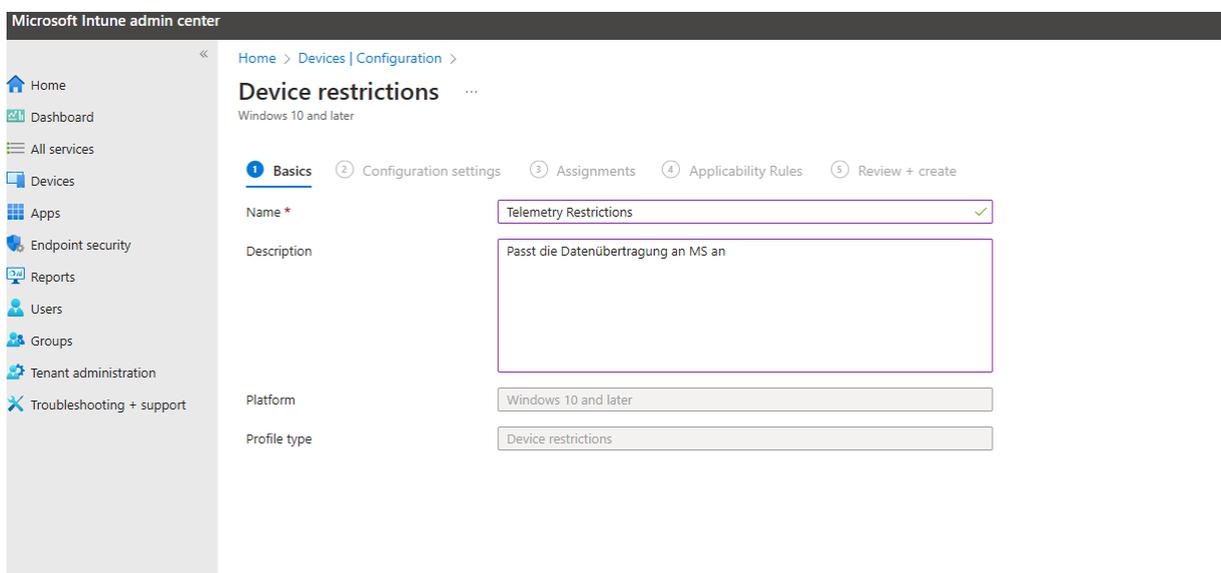
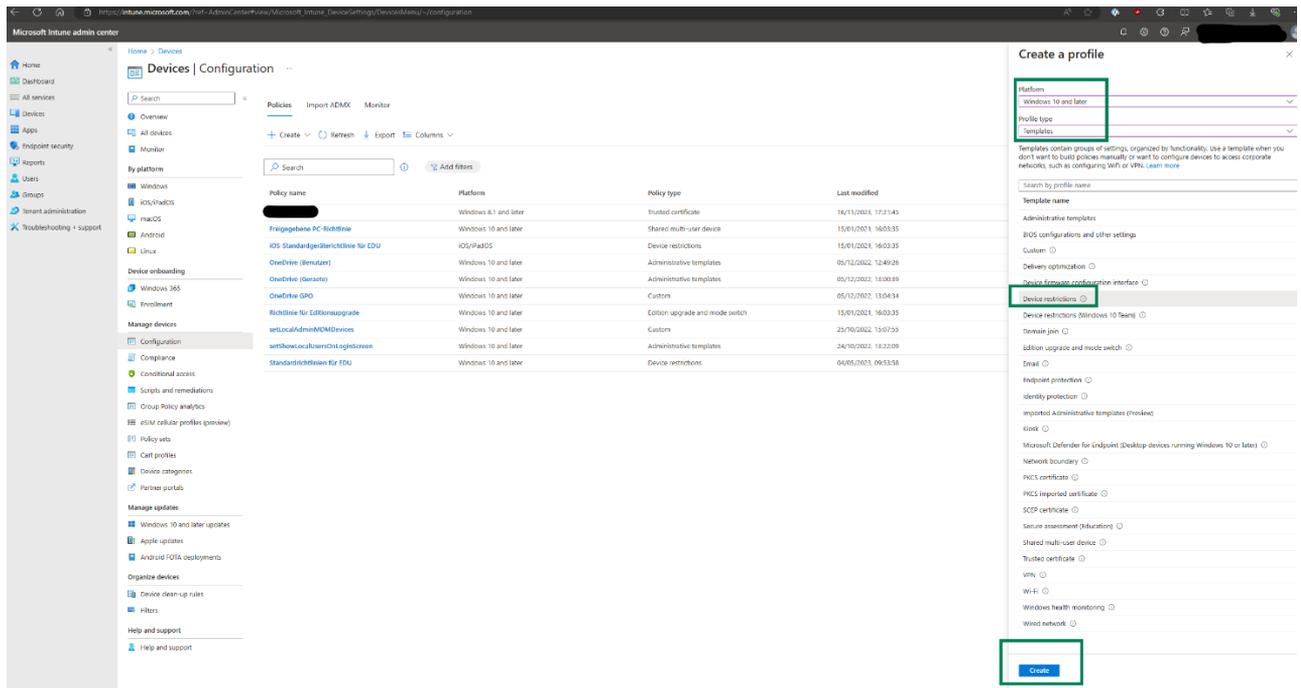
1 Office on the web.....	2
2 Office 365 Apps	5
2.1 Setzen des Update Channels für MS365 Apps auf monthly Enterprise Channel:.....	5
2.2 Datenschutzeinstellungen	5
3 Office 2021 LTSC.....	10

1 Office on the web

In den nächsten Schritten wird eine Policy für die Intune Geräteverwaltung erstellt, die die Telemetry- und Privacy-Settings der Endgeräte anpasst und so unerwünschte Datenströme zu MS unterbinden soll. Die Policy wird „Telemetry Restrictions“ genannt.

Intune Configuration Profile - Windows Diagnostics Data (All Devices Setting):

Devices -> Configuration -> Create New Policy (Name: Telemetry Restrictions):



In den Configuration Settings der Policy werden unter dem Reiter „Privacy“ folgende Einstellungen vorgenommen:

Device restrictions

Windows 10 and later

Printer

Privacy

Privacy experience ⓘ	Block	Not configured
Input personalization ⓘ	Block	Not configured
Automatic acceptance of the pairing and privacy user consent prompts ⓘ	Allow	Not configured
Publish user activities ⓘ	Block	Not configured
Local activities only ⓘ	Block	Not configured

Define information that all apps on the device can access. You can define exceptions on a per-app basis using "Per-app privacy exceptions".

Account information ⓘ	Not configured
Background apps ⓘ	Not configured
Calendar ⓘ	Not configured
Call history ⓘ	Not configured
Camera ⓘ	Not configured
Contacts ⓘ	Not configured
Email ⓘ	Not configured
Location ⓘ	Not configured
Messaging ⓘ	Not configured
Microphone ⓘ	Not configured
Motion ⓘ	Not configured
Notifications ⓘ	Not configured
Phone ⓘ	Not configured
Radios ⓘ	Not configured
Tasks ⓘ	Not configured
Trusted devices ⓘ	Not configured
Feedback and diagnostics ⓘ	Not configured
Sync with devices ⓘ	Not configured

In den Configuration Settings der Policy werden unter dem Reiter „Reporting and Telemetry“ folgende Einstellungen vorgenommen:

Device restrictions

Windows 10 and later

Basics Configuration settings Assignments Applicability Rules Review + create

- App Store
- Cellular and connectivity
- Cloud and Storage
- Cloud Printer
- Control Panel and Settings
- Display
- General
- Locked Screen Experience
- Messaging
- Microsoft Edge Legacy (Version 45 and earlier)
- Network proxy
- Password
- Per-app privacy exceptions
- Personalization
- Printer
- Privacy
- Projection

Reporting and Telemetry

Share usage data Diagnostic data off

Send Microsoft Edge browsing data to Microsoft 365 Analytics Not configured

Telemetry proxy server e.g. 249.168.246.106:100 or [2001:4898:4010:4013:95c1:a8b2:953c:c633];1...

Die getroffenen Einstellungen werden auf die Gerätecollection „All devices“ angewendet:

Home > Devices | Configuration >

Device restrictions

Windows 10 and later

Basics Configuration settings Assignments Applicability Rules Review + create

Included groups

Add groups Add all users Add all devices

Groups	Group Members	Filter	Filter mode	Edit filter	Remove
All devices		None	None	Edit filter	Remove

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more about excluding groups.](#)

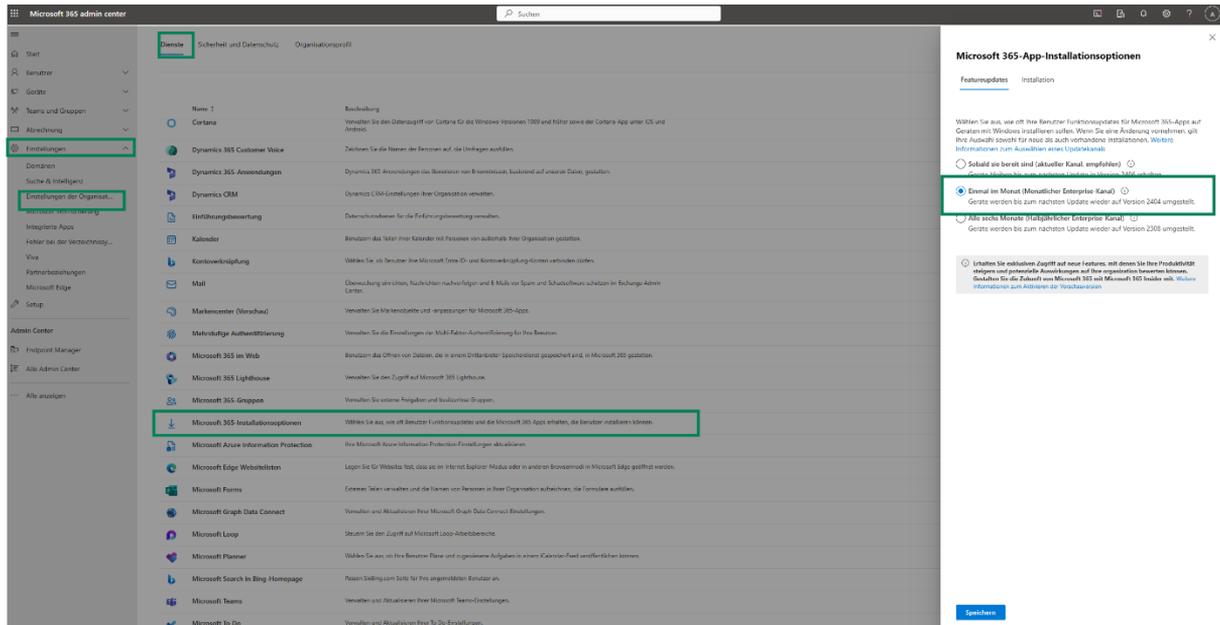
+ Add groups

Groups	Group Members	Remove
No groups selected		

2 Office 365 Apps

2.1 Setzen des Update Channels für MS365 Apps auf monthly Enterprise Channel:

Alle>Einstellungen>Einstellungen Organisationseinstellungen>Dienste>Microsoft 365-Installationsoptionen:



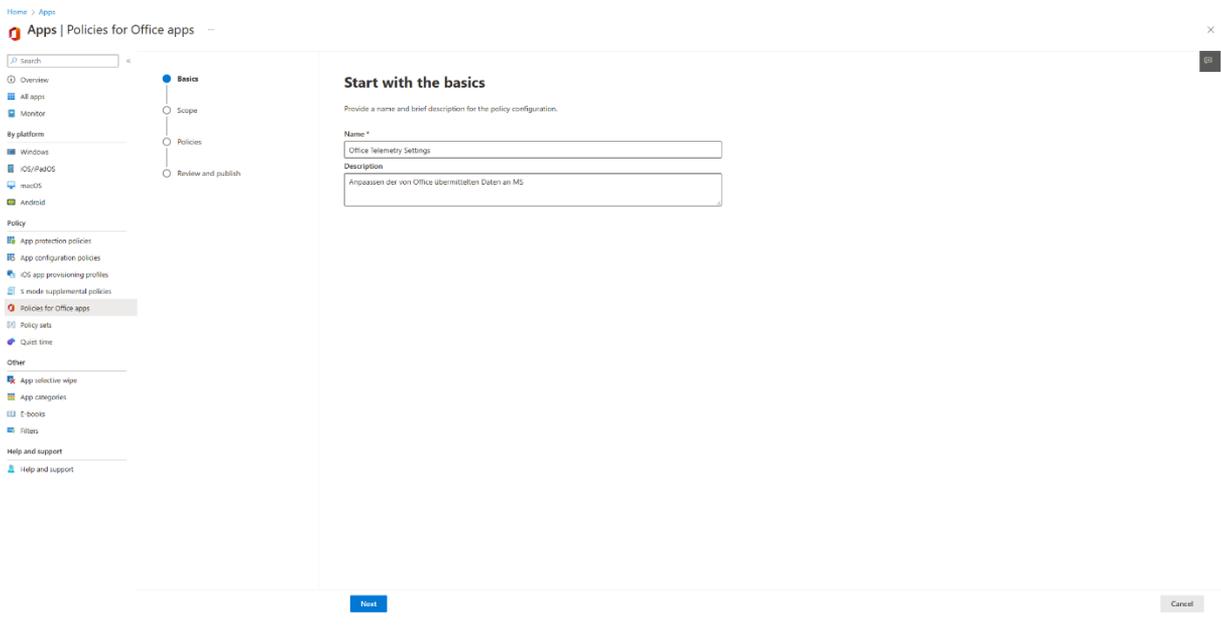
Der Kanal wird auf monthly umgestellt, damit die Updates von Microsoft nicht sofort angewendet werden, sondern mit einer Verzögerung von einem Monat.

2.2 Datenschutzeinstellungen

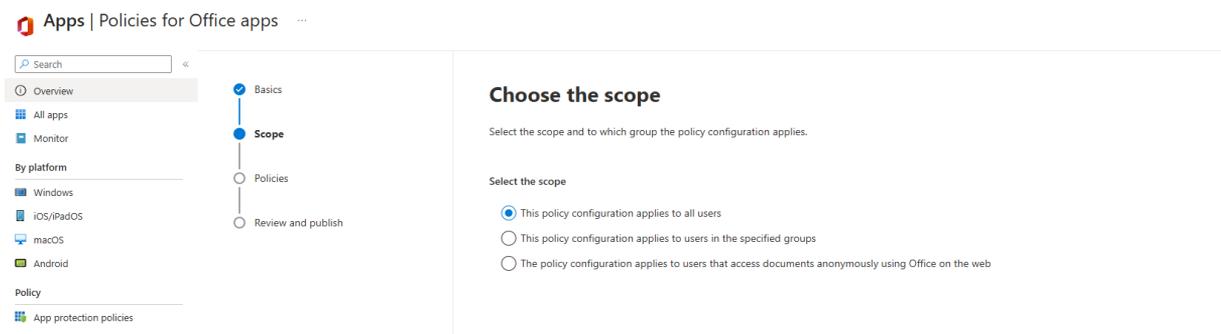
In den nächsten Schritten wird eine Policy für die Applikationen von Office365 erstellt, die die Telemetry Settings der Endgerätebenutzer anpasst und so unerwünschte Datenströme zu MS unterbinden soll. Die Policy wurde „Office Telemetry Settings“ genannt.

Policy for Office Diagnostics Data (User Settings -> All USers):

Apps -> Policies for Office Apps -> Create:

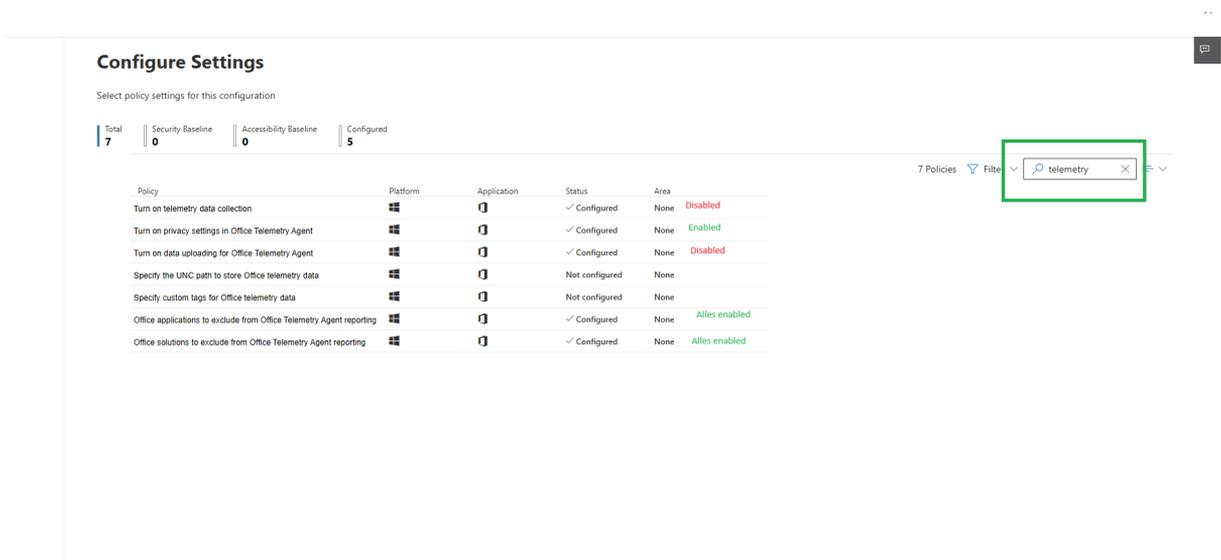


Die Policy wird für alle User angewendet:



Das Schlagwort „Telemetry“ offenbart folgende Konfigurationsmöglichkeiten:

Die getroffenen Konfigurationen wurden aus Platzgründen in rot und grün dargestellt in der Liste verschriftlicht:



Extra angeführt „Office applications to exclude from Office Telemetry Agent reporting“:

The screenshot shows the 'Configure Settings' page for 'Policies for Office apps'. The main table lists several policies, with the following data extracted:

Policy	Platform	Application	Status	Area
Turn on telemetry data collection	Windows	Office	Configured	None
Turn on privacy settings in Office Telemetry Agent	Windows	Office	Configured	None
Turn on data uploading for Office Telemetry Agent	Windows	Office	Configured	None
Specify the UNC path to store Office telemetry data	Windows	Office	Not configured	None
Specify custom tags for Office telemetry data	Windows	Office	Not configured	None
Office applications to exclude from Office Telemetry Agent reporting	Windows	Office	Not configured	None
Office solutions to exclude from Office Telemetry Agent reporting	Windows	Office	Not configured	None

The right-hand panel, titled 'Office applications to exclude from Office Telemetry Agent reporting', provides a detailed configuration interface. It includes a 'Configuration setting' dropdown menu set to 'Enabled', and a section for 'Additional setting' with various solution-related dropdowns (Word, Excel, PowerPoint, Outlook, Access, Project, Publisher, Visio, OneNote), all of which are currently set to 'Enabled'. A large question mark icon is visible in the background of this panel.

Extra angeführt „Office solutions to exclude from Office Telemetry Agent reporting“:

Configure Settings

Select policy settings for this configuration

Policy	Platform	Application	Status	Area
Turn on telemetry data collection	☑	☑	✔ Configured	New
Turn on privacy settings in Office Telemetry Agent	☑	☑	✔ Configured	New
Turn on data uploading for Office Telemetry Agent	☑	☑	✔ Configured	New
Specify the UNC path to store Office telemetry data	☑	☑	Not configured	None
Specify custom tags for Office telemetry data	☑	☑	Not configured	None
Office applications to exclude from Office Telemetry Agent reporting	☑	☑	✔ Configured	New
Office solutions to exclude from Office Telemetry Agent reporting	☑	☑	Not configured	New

Office solutions to exclude from Office Telemetry Agent reporting

This policy setting allows you to prevent telemetry data for Office solutions from being reported to Office Telemetry Dashboard.

If you enable this policy setting, Office Telemetry Agent does not upload telemetry data for the specified Office solutions to Office Telemetry Dashboard.

If you disable or do not configure this policy setting, Office Telemetry Agent uploads telemetry data for all available solution types.

Configuration setting

Enabled

Additional setting

Office document files: Enabled

Office template files: Enabled

COM add-ins: Enabled

Application-specific add-ins: Enabled

Web Add-ins: Enabled

Create:

Review configuration and create

Review the settings for your policy configuration and then select Create.

Basics

Name: Office Telemetry Settings

Description: Anpassen der von Office übermittelten Daten an MS

Scope: All users

Policies

5 policies configured

Security Baseline: 0 baseline policies configured

Accessibility Baseline: 0 baseline policies configured

Buttons: Back, Create, Cancel

Schlagwort „Diagnostic“:

Level wurde auf „Required“ gesetzt, damit nur die minimalen, erforderlichen Datenströme an MS gesendet werden, um die Stabilität der MS Produkte zu gewährleisten.



Alternativ/Zusätzlich können über ein Konfigurationsprofil noch folgende Registry Keys gesetzt werden:

Windows

Registry Editor Version 5.0

[HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\osm]

"Enablelogging"=dword:00000000

"EnableUpload"=dword:00000000

3 Office 2021 LTSC

Analog zu den MS365 Client settings können für die LTSC Version von Office die gleichen registry keys gesetzt werden:

Windows

```
Registry Editor Version 5.00 [HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\osm]
```

```
"Enablelogging"=dword:00000000
```

```
"EnableUpload"=dword:00000000
```

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Bildung, Wissenschaft und Forschung
Gruppe PräS/C
Minoritenplatz 5, 1010 Wien
Tel.: +43 1 531 20-0
Wien, Juli 2024