Konverion

Microsoft 365Checker Manual

Version 8

Konverion UG (limited liability)
Markelstrasse 48
12163 Berlin
Managing Director: Jörg Schanko

Local court Berlin-Charlottenburg
HRB: 195062 B
ST-No: 29/392/30664
VAT ID: DE317517149

Bank details
Fyrst Postbank Ndl der Deutsche Bank
IBAN: DE23 1001 0010 0064 6861 40
BIC: PBNKDEFFXXX

Content

Foreword

The Microsoft 365 Checker is a tool designed primarily to help works council members, but also compliance officers, to monitor the configurations made in the numerous components of Office 365.

For example, it is easy to determine whether the regulations laid down in a company agreement are also consistently implemented. The Microsoft 365Checker only needs read-only access to the respective Microsoft 365Tenant. The extracted configurations are stored on the local PC in an encrypted database. In this way, the configuration statuses at different times can be compared and differences made visible.

To access Office 365, the Microsoft 365Checker uses so-called PowerShell modules. PowerShell is the scripting language developed by Microsoft to help administrators automate frequently recurring administrative tasks.

In order to be able to use the Microsoft 365 Checker sensibly, you need either a user account with sufficient administrative permissions or a registered application in Entra ID in your Microsoft 365 tenant.

Note on older versions of the checker (7.x)

Microsoft has announced two major changes that affect the functionality of the checker.

1. The AzureAD and AzureAD Preview PowerShell modules will be retired in March 2025. The "Microsoft Graph PowerShell" modules serve as a replacement. These require the registration of an application in Entra ID. For the checker, we have dispensed with the use of the Microsoft Graph PowerShell modules, and access settings directly via the Microsoft Graph. This increases speed and reduces complexity. With version 8 of the checker, the AzureAD or AzureAD Preview PowerShell modules can already be dispensed with.
2. All user accounts with administrative permissions will require multi-factor authentication MFA from the beginning of 2025 (already implemented now for access to any administrative websites).
   This means that the "encapsulated mode" of the older Checker versions can no longer work, as MFA always requires an interactive login. In order to offer functionality comparable to the encapsulated mode, you can switch to a certificate-based login from version 8 onwards.

Version 8 of the Checker also supports all the possibilities of the older versions, as long as this is technically possible. However, it makes sense to switch to the graph-based functions now for speed reasons alone.

Telemetry

Telemetry is an excellent way to collect the necessary data to fix a bug in a program and improve its functionality.

However, since the Microsoft 365Checker reads sensitive information about the configuration of an Microsoft 365Tenant, we have completely dispensed with telemetry. In other words: the Microsoft 365Checker "does not phone home". Neither for product improvement, nor for license control, nor otherwise. The only contact to our server is made by the checker at startup to see if a new version is available and if you download the manual by clicking the Question mark in the top left corner.

But not using any kind of telemetry also means that we depend on user feedback to improve the Microsoft 365Checker.
So if you find errors, a feature is not what you want it to be, or it is not available - send an email to support@konverion.de. THANK YOU!

Licensing

To determine if Microsoft 365Checker meets your expectations and provides the features you need, you can try it for 30 days. No registration or similar is necessary. During the test period, all functions are available to you without restriction.

After 30 days, you will not be able to create new reports. However, you can still access reports that have already been created.

To continue to generate new reports after the trial period expires, you must purchase a license of Microsoft 365Checker. You can use the order form available on our website for this purpose.

With the purchase of a license you get the right to use Microsoft 365Checker on as many PCs as you like. The license is also not limited to a certain number of users.

After receipt of the order we will send you a license file. You store this license file in the data directory ("c:\data\Office365Checker") on each PC on which Microsoft 365Checker is to be run.

You can find more information about licensing on our website.

Preparation

In order for the Microsoft 365 Checker to be able to read configurations in your Microsoft 365 tenant, it needs appropriate permissions and (currently) some PowerShell modules.

The easiest way to do this is to use the Global Reader role predefined in Microsoft 365. This role is allowed to read all settings in Microsoft 365, except for eDiscovery searches and Data Subject Requests in the GDPR dashboard. To evaluate the audit logs, assign the Audit Manager roles to the user account in Microsoft Purview. The entries in the audit log can then also be used to determine whether eDiscovery searches or similar have been carried out.

To use the Microsoft 365 Checker, it makes sense to create a separate account in Microsoft 365 and assign the necessary rights to it. In this way, the use of the checker can also be traced in the Microsoft 365 event log.

Within the scope of this manual, the accounts "braudit@zusenberg.de", or brauditMFA@zusenberg.de , are used.

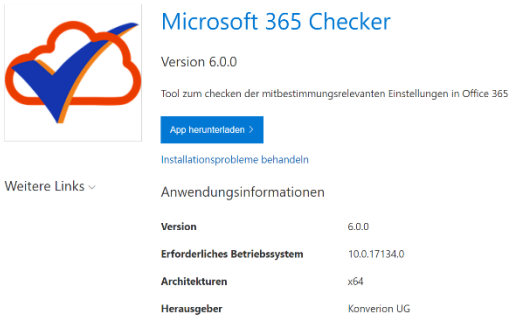
To configure the checker to use the Microsoft Graph programming interface or certificate-based login, see the section "Settings – Graph" or "Settings – Certificate".

For the initial installation of the necessary PowerShell modules, you must also have administrator rights on the local PC. However, this is only necessary for the installation of the "NuGet" PowerShell modules. These are needed to find and download modules in the Microsoft PowerShell Gallery (https://www.powershellgallery.com/). To run the Microsoft 365 Checker, you don't need these admin privileges.

If you only want to import, view, and compare reports, you don't need to install the PowerShell modules.

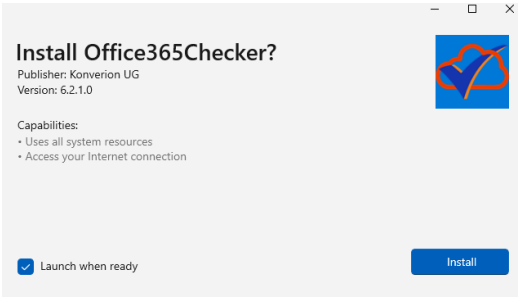
Installation

Start the installation of the Microsoft 365 Checkers by calling the URL
https://www.konverion.de/Microsoft365Checker/index.html



Click on “App herunterladen” to download the software package.

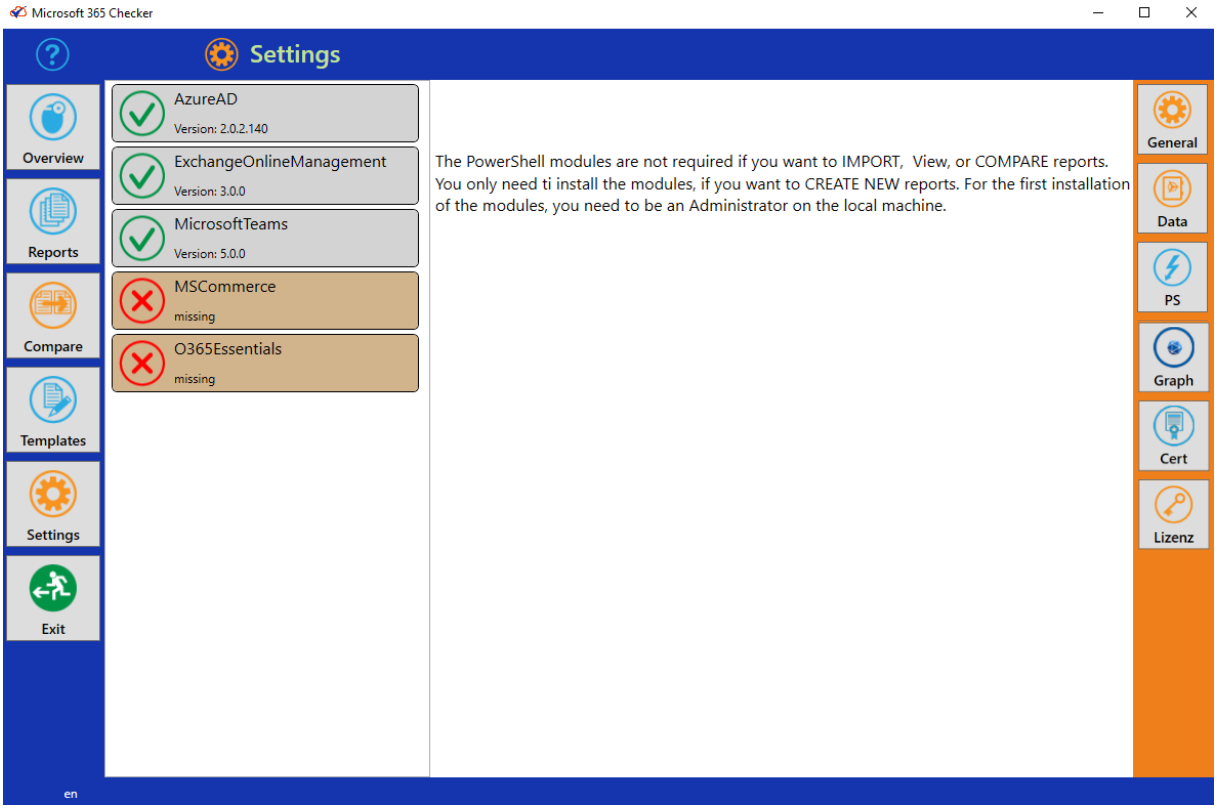
After download click on “Open file”.



Click on “Install”

During installation, Microsoft 365Checker creates a directory "c:\Data\Office365Checker". The encrypted database (Office365Checker.db3) and the log file (Log.txt) are created in this directory. In addition, a subdirectory "Reports" is created in which all exported reports are saved.

After the first start, the Microsoft 365Checker first checks whether all required Powershell modules are available on the local PC:



If the modules you desire / need are not yet installed on your PC, click on "Install". For the installation of Powershell modules you need administrator rights on the local PC. The “Install” Button is only visible, if not all required modules were found on your PC.

There are three core and two optional PowerShell Moduls.
The core modules are:

- AzureAD
- ExchangeOnlineManagement
- MicrosoftTeams

The two optional modules are described in the following chapters.

All installed PowerShell modules are stored in “C:\data\Office365Checker\PS”.

When all necessary powershell modules are installed you can start working with Microsoft 365Checker.

“MSCommerce” PowerShell Module

The "MSCommerce" PowerShell module can show you the settings for the so-called "self-service purchases".

If self-service purchases are allowed, users can install certain products without the involvement of the IT department. For fee-based products, these can be paid for with a private credit card.

You can find out which products are eligible for self-service purchases in the "MSCommerce" table in the "Readable settings" appendix.

When using the "MSCommerce" PowerShell module, please note that it always requires a separate login. So if you install the module and integrate the self-service purchases into a report, you will be asked to log in again and again when you create the report.

Due to the requirement of an interactive login, the "MSCommerce" module cannot be used with certificate-based login and cannot be used in encapsulated mode.

It is to be hoped that Microsoft will adapt this module to the standards of the other PowerShell modules in the future, so that separate authentication is no longer necessary.

If you want to read the settings for self-service purchases, click on the "MSCommerce" switch. The module is then installed and can then also be found in the folder "c:\data\office365checker\PS". If you have set up the checker to use the Microsoft Graph API, you do not need to install the MSCommerce PowerShell module, as the settings can be read via the Graph API.

"O365Essentials" PowerShell Modul

This module belongs to the optional PowerShell modules because it uses undocumented Microsoft application programming interface (API) functions and does not come from Microsoft itself.

Currently, this is the only way to read the organization settings in an automated way.

O365Essentials" is an OpenSource project of the company "EvotecIT". The source code can be found on GitHub https://github.com/EvotecIT/O365Essentials .

The permanent function of this module cannot be guaranteed due to the undocumented functions used.

Organization settings include data location, settings for Forms, Bookings, MyAnalytics., etc. For the complete list of organization settings that can be read, see the appendix "Readable settings" under "Organization settings".

If you want to read out the organization settings, click on the "O365Essentials" button. The module will then be installed and can also be found in the "c:\data\office365checker\PS" folder afterwards.

"AzureADPreview" PowerShell Module.

Note: The "AzureADPreview" PowerShell module will be retired on March 30, 2025. If you are using the Microsoft Graph programming interface for the checker, you do not need to install the module.

The AzureADPreview PowerShell module is currently only necessary to read the extended properties of Azure AD Administrative Units. IF administrative units are set up, can be detected by the AzureAD module. The assigned members and administrators, as well as the number of users, groups and devices contained in the management unit and, if applicable, the dynamic creation rule can only be read via the Preview module.

If you do not use administrative units there is currently no reason to install the AzureADPreview module. However, in one of the next versions of the checker, the "Privileged Identity Management (PIM)" will also be readable via this module.

If you click on the button for the AzureADPreview module, it will be installed after a security prompt and the AzureAD module will be uninstalled. If you have previously created a report that includes

Azure AD, it may not be possible to delete the AzureAD module because files are still in use. In this case, exit the checker and delete the "c:\data\office365checker\PS\AzureAD" directory manually.

You can always reinstall the AzureAD module by clicking the appropriate button. The AzureADPreview module will then be uninstalled again.

General procedure

To make working with Microsoft 365Checker as easy as possible, follow these steps:

Use "Templates" to define which Microsoft 365service configurations you want to control. You can create any number of templates for different requirements.
The creation of templates is described in chapter "Create templates“

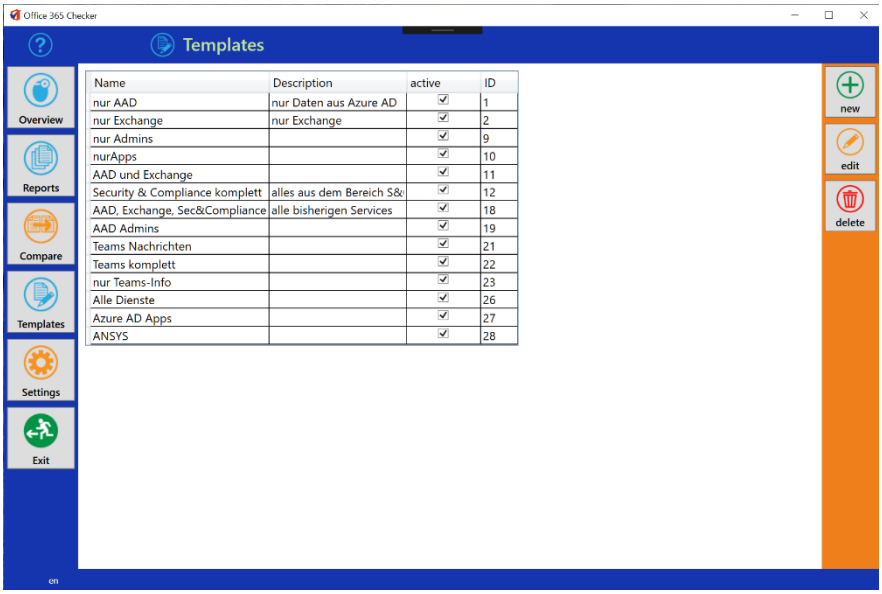
1) Once you have defined your templates, you can create a new report based on one of your templates in the "Reports" section.
   The creation of reports is described in "Generate reports".
2) Once a report has been created, you can save it as a Word file or print it, for example, to compare it with the configuration defined in the company agreement.
3) To detect changes over time, you can compare reports created at different times in the "Compare" section. The Microsoft 365Checker then displays the changes it has detected.
   The procedure is described in "Compare reports".

Create templates

Templates let you control which Microsoft 365service configurations you want to combine into a report. For example, you can create a template to summarize the configuration of all services used in one report, but you can also create a separate template for each individual service such as Exchange, Azure Active Directory, etc. You can also include a single function in a template, for example, to create a separate report for the authorization concept in Office 365.

The number of templates is not limited.

To work with templates, select the Templates 

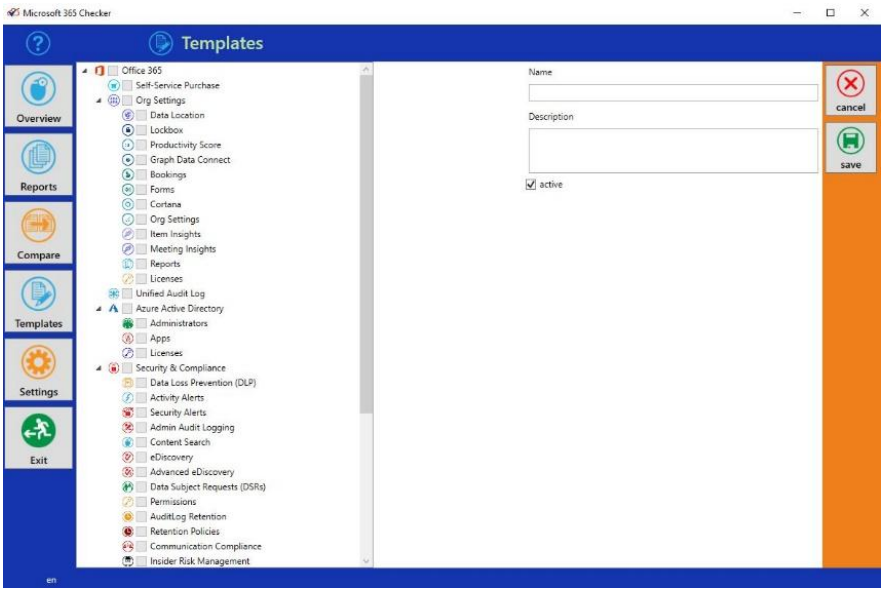


A view of the templates already defined is displayed:

If you click on an existing template in the list, you will see which service configurations are combined in this template.

Create a new template

To create a new template, click on the "New" function button.



In the tree structure on the left side, all configurations that Microsoft 365Checker can read are displayed. Select the desired services that you want to summarize in a report. Then give your template a name and a description. You can use the "active" checkbox to specify that this template is no longer offered when creating a new report.

Click on "save" to create your new template.

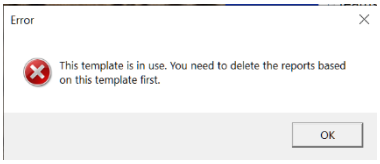
Edit templates

With "Edit template" you can change the name, description and status of a template (active or inactive). You cannot change the services once they have been combined in a template, otherwise the comparison of individual reports becomes inconsistent.

To edit a template, select it from the list of templates and click on "change".
After you have made the desired changes, click on "save".

Delete templates

You can delete templates on the basis of which no reports have yet been created.
To do this, select the template to be deleted from the list and click "delete". The template is deleted and disappears from the list.

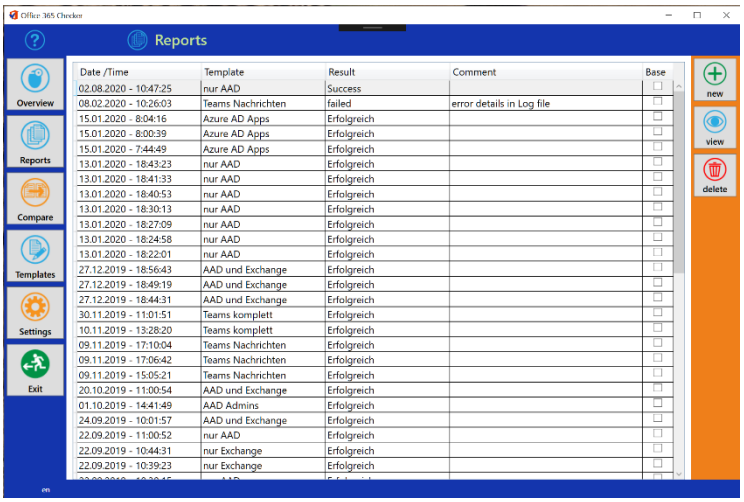


If reports have already been created with the selected template, the system displays a corresponding message:

You must therefore first delete the reports based on this template before you can delete the template. The procedure is described under "Delete report".

Generate reports

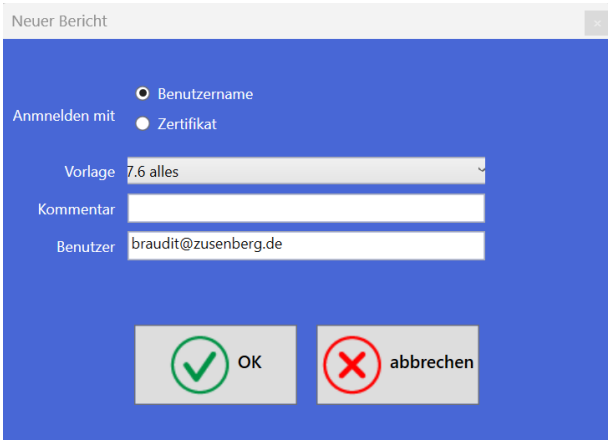
The configurations read from Microsoft 365are compiled in reports. To work with reports, click on the "Reports" section.



Here you can see a list of the reports already created. The date and time of creation and the name of the template on which the reports are based are displayed. In the column "Result" you can see whether the report was created successfully. If you have already entered comments for a report, these will also be displayed. In the "Base" column, you can see which report you have marked as the basis for comparison.

Create a new report

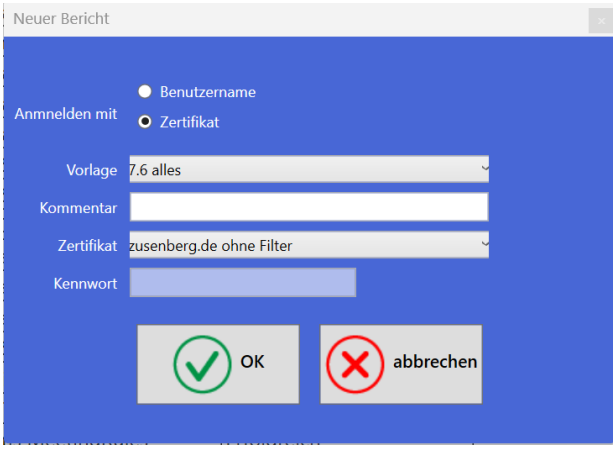
The dialog box for creating new reports has changed to reflect the new features:



Note:For the time being (probably until the beginning of 2025), the "old" dialog of Checker version 7.x is still available. To get the old dialog for creating new reports, press the left Shift key and then click on the plus sign for a new report.

When logging in with a username, an account with multi-factor authentication activated will be required from the beginning of 2025. The password is prompted interactively after you have clicked on "OK".

If you change the login to "Certificate", the dialog box changes:



The "Certificate" list lists all created login files (see: "Setting Up Certificate-Based Login")

Select the desired login file and enter the corresponding password.

The checker then uses the certificate information stored in the login file to log in to PowerShell or the Microsoft Graph. When logging in with a certificate, a user account is no longer required.

You'll see the rotating Microsoft 365 Checker logo and a "Generating report" message.

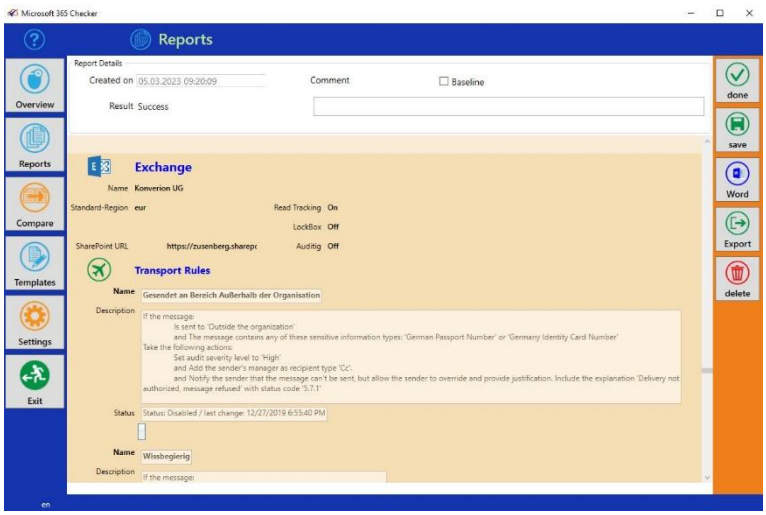
Depending on the number of configurations to be read, creating a report can take several minutes to a few hours.

When the report generation is finished, the list of existing reports is displayed again. The newly created report appears in the top row.

To view the report, select the report in the list and click View.

View reports

To view any report from your list of existing reports, select the desired report from the list in the "Reports" section and click "View".



The upper part of the display area shows the details of the report. These are the date and time of creation, the status whether the report was successfully created, the comment on this report and the checkbox "Basis of comparison". This is explained in the section "Determine basis of comparison".

In the lower part of the display area you see the actual report with the configurations read out. What exactly is displayed here depends on the template you have chosen to create the report. However, the general structure is always the same:

A header area with general information and the icon of the Microsoft 365service that was read (in the picture above: Exchange). This is followed by sections for the configurations that have been read

("Transport Rules" in the screen above), which are also marked with an icon. Within the sections then - depending on the configuration read, one or more paragraphs with the specific configurations.

You can scroll through the entire report using the scroll bar.

Filter reports

If you select a report in the list of reports and then click the 

button, the report to be displayed will be filtered.

In a filtered report, the following information is hidden:

- all unused administrator roles from Azure Active Directory (roles without members).
- all apps registered in Azure AD that do not have application permissions on the Microsoft Graph
- all security notifications in Security & Compliance that are predefined by Microsoft
- all unused permission roles from the Compliance area (roles without members)
- all “AdvancedRules” from Data Loss Prevention.

Filtering can shorten reports, sometimes significantly, without omitting relevant information for co-determination or privacy.

When you view a filtered report, the appropriate icon appears in the header.

When you export a filtered report or output it as a Word document, only the filtered data is included.

The filter does not remove any data from a report, it is just not displayed in this view.

Determine basis of comparison

If, after reviewing a report, you have determined that the configurations read are as they should be - i.e. as specified in a company agreement, for example - you can specify this report as a basis for comparison by selecting the "Baseline" checkbox and then clicking "Save".

This means that this report is always displayed at the top of the "Compare" section. For more details, see the "Compare reports" section.

Save report as Word document

To save a report as Word document, select the desired report in the "Reports" section and then click "View". The selected report is then displayed and you can create a word file it by clicking on the "Word" button. A Word file is created from the report and saved in the "c:\Data\Office365Checker\Reports" folder.

The file name of the report is composed of the date and time of creation, for example "18-09-2019_13-52-11.docx" for a report created on 18.09.2019 at 13:52.11.

You can now open the report in Microsoft Word and print it if necessary.

Delete report

To delete a report, select the desired report in the "Reports" section and then click "Delete". A confirmation prompt appears asking whether you really want to delete the selected report:

Once deleted reports cannot be recovered. So before you delete reports, export the report or create a backup of the database (see "Backup" in the "Settings" section).

You can also delete a report when you are in the report view. There is also a "delete" button here. Here, too, the selected report is permanently and irretrievably deleted.

Any existing exports of the deleted report are not deleted.

Export report

You can export reports to import them again in another installation of Microsoft 365Checker.

This allows you, for example, to create reports by the IT department, export them and make them available to the works council. The latter can now import the reports without needing an account with read permissions for the Microsoft 365configuration. The option provides an alternative to using the encapsulated mode.

To export a report, select the desired report in the "Reports" area and then click "View". The selected report will then be displayed. Click the "Export" button. You will see a dialog box where you can specify where the export file will be saved. The default name is "Export.tra". You can change the name as you like, the file extension ".tra" will always be kept.

The export file is automatically encrypted and checksummed, so it is not possible to modify the exported reports. Any changes to the contents of the exported file will make it impossible to import the file again.

Import report

To import exported reports, click Import in the Reports section. A dialog box will appear where you can select the file to import (file extension ".tra"). Confirm the selection with "Open".

The file will be decrypted and compared with the contained checksum. If the check is successful, the report will be imported. Otherwise, you will receive an error message that the file is corrupted.

The imported report is marked with "[Import]" in the comment field.

In addition to the report, the template used to create the report is also installed. The original template name will have "[Import]" added to it. For example, if the original template name was "All Services", after the import you will find it in the list of templates under the name "[Import] All Services".

Reports cannot be imported into the same instance of Microsoft 365Checker from which they were exported.

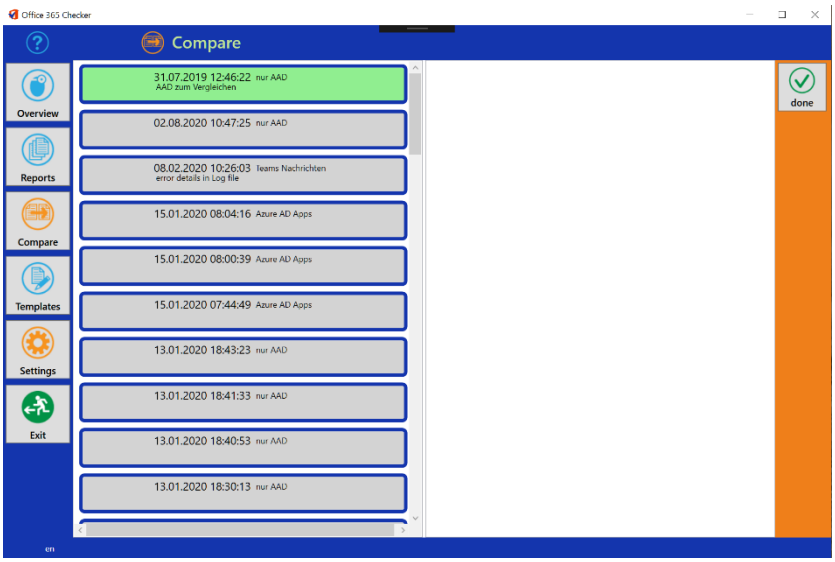
Tip:

If you want to compare imported reports with each other, make sure that the reports were all exported from the same computer. Each installation of Microsoft 365Checker has its own ID that is exported along with it to distinguish the templates. This way, when importing multiple reports created with the same template and on the same PC, the corresponding template is installed only once and you can compare these reports with each other.

If the reports come from different PCs, the templates will be imported with each report, even if they have the same name. Reports based on different templates cannot then be compared with each other.

Compare reports

To easily track changes in the configuration in your Microsoft 365Tenant, you can compare reports once they have been created. The Microsoft 365Checker will show you the differences found.
You can only compare reports that were created using the same template.

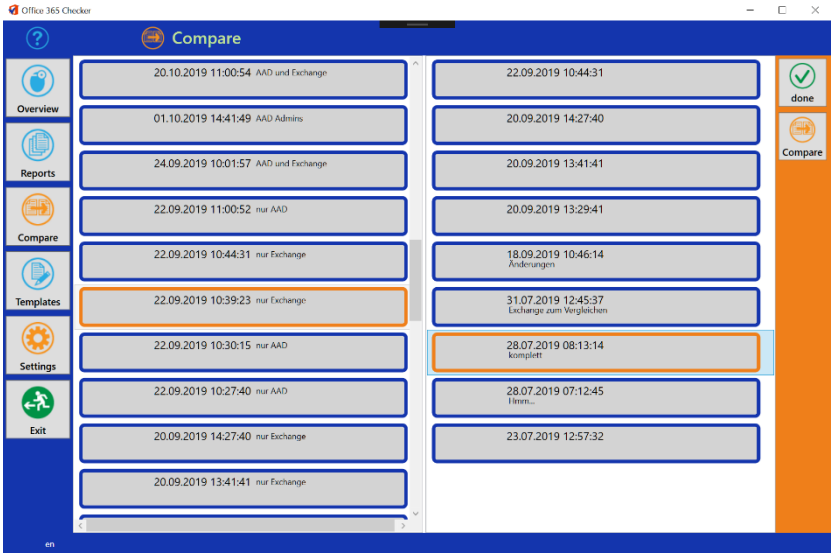


To compare reports with each other, select the "Compare" section.

The system displays a list of all reports that have already been successfully created. For each report, you can see the date and time of creation, the template used, and any comments.

If you have already defined a report as the basis of comparison, this report is always displayed at the top of the list and has a green background. From the list, select the report with which you want to compare another one. The selected report will have an orange frame.

The right column of the display area will then show you all reports based on the same template as the selected report.



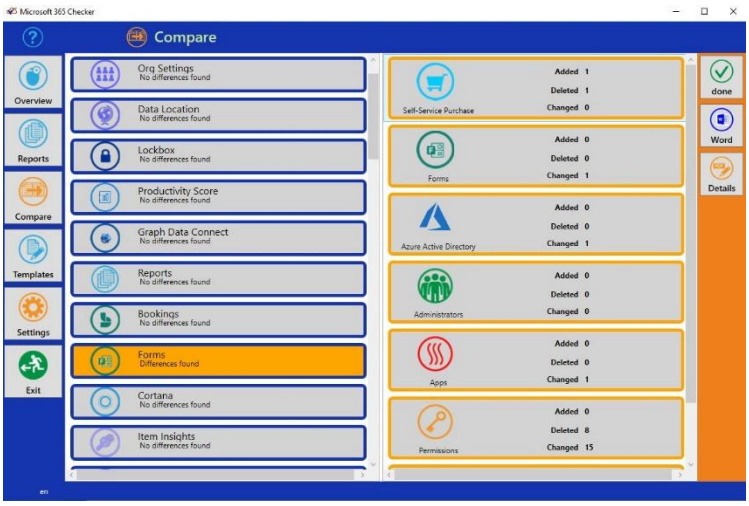
From the list on the right, select the report with which the orange marked report of the left list is to be compared.

The selected report is also outlined in orange and a "compare" function button appears.

Now click on "compare" to compare the selected reports.

The Microsoft 365Checker now displays the result of the comparison:

The list on the left side shows all services whose configuration has been recorded in the reports. If no deviations were found for a service in the configurations, the service is displayed with a grey background and the remark "no differences found".



If differences were detected in the two compared reports for a service, the service is given an orange background and the remark "Differences found".

For these services, the differences found are then displayed in the right-hand column.

For each service you can see, how many informations were added, deleted, or changed.

Compare Details

With a click on the ”Details” button, you can create a PDF-document which lists the details of the changes.

Example:

Self-Service Purchase

```
Deleted: {
 "product": "Power BI Premium (standalone)",
 "setting": "Enabled",
 "productID": "CFQ7TTC0KXG7"
}
Added: {
 "product": "Power BI Premium per user",
 "setting": "Enabled",
 "productID": "CFQ7TTC0KXG7"
}
```

In “Self-Service Purchase” the product “Power BI Premium (standalone)” was deleted, and

the product “Power BI Premium per user” was added.
As you can see, the product-ID has not changed, so Micxrosoft only renamed this product.

Export comparison

The results of the comparison can be saved in a Word file using the "Export" function button. Like reports, the Word files of the comparisons are stored in the folder "c:\Data\Office365Checker\Reports". The file name is "Comparison_ *Date&Time", for* example "Comparison_24-09-2019_13-55-20.docx" for a comparison that was saved on 24.09.2019 at 13:55.20.

Settings

The category "Settings" is currently divided into six areas, which are described below.

General

In this area you can define the standard user that is automatically transferred to the input mask when a new report is created. If you make changes here, do not forget to click on "save". Otherwise the changes are discarded.

In the “Encapsulated Mode” pane, you can create the Encryption File for Encapsulated Mode as described in the "Creating the Office365Checker.locked File" section.

In the "Printer" section you can preset a default printer. However, the default printer is not currently used.

With the setting "Use proxy settings (beta)" you can specify that the Microsoft 365Checker uses the proxy settings defined for Internet Explorer to connect to the Internet. The function is still in beta stage and not fully tested.

If you encounter problems when using this feature, please contact support@konverion.de.

In the "Info" section you will find information about the current version number of the program and the database. This information may be requested from you in case of support.

Data

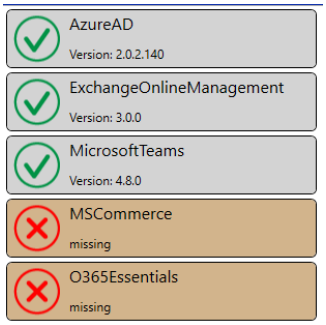
Here you can see the current path to the database (Office365Checker.sdf) If necessary, you can move the database to another hard disk or directory by clicking the "move" button. However, as long as there are no weighty reasons, you should leave the database where it is.

Via "Change" you can change the selected database, for example to access a previously saved database (see Data Backup).

You can create a backup copy of your database using the "Backup" button. If you click on the button, a dialog box appears in which you can specify where the backup copy is to be stored. The default name for the backup copy is Office365Checker_Date&Time.*sdf*, where *Date&Time is the* current date and time of the backup. You can change the name as you wish.

PS (PowerShell)

This section provides an overview of whether all necessary PowerShell modules for the Microsoft 365Checker are installed. If this is not the case, you can start the installation from here.



In this example, the modules for

- Azure Active Directory
- Exchange Online Management, and
- Microsoft Teams

are installed. The optional modules “MSCommerce” and “O365Essentials” are not installed.

You can install (or update) the modules by clicking on the module.

For the installation of PowerShell modules administrative rights on your local PC are required.

Microsoft Graph

Starting with version 8 of the checker, the Microsoft Graph application programming interface (API) can be used instead of the PowerShell modules "AzureAD", "AzureAD Preview" and "MSCommerce" to read the corresponding configurations. The use of the Microsoft Graph has 3 main advantages:

- the Microsofft Graph is constantly being developed,
- the Microsoft Graph supports modern authentication, and
- the reading of the configurations is considerably faster (about a factor of 5)

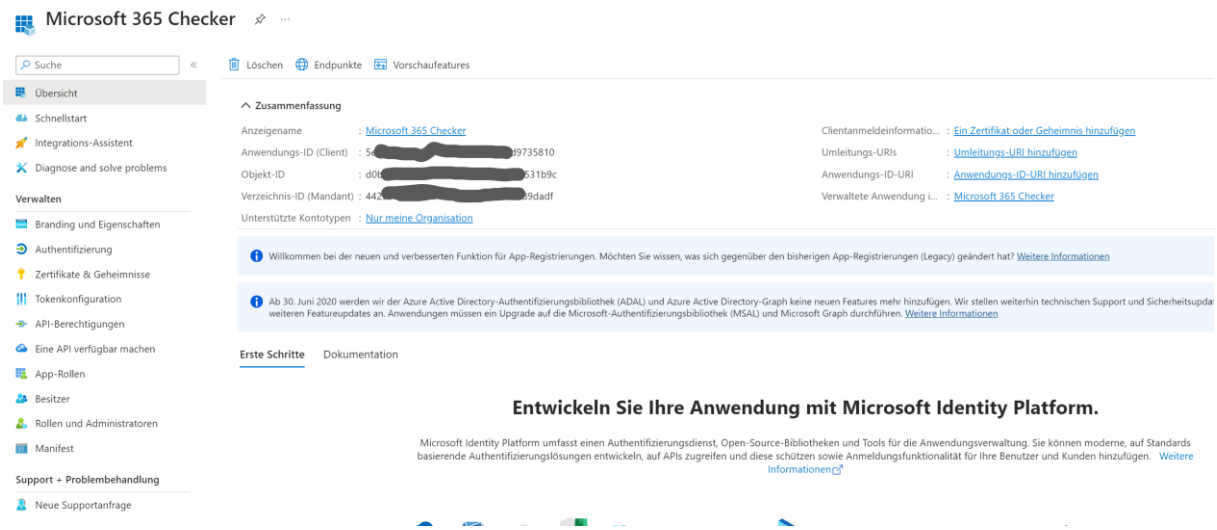
The disadvantage is that to use the Microsoft Graph and the certificate-based login in Entra ID, you have to register an application to provide the checker with the necessary permissions. This no longer requires an account with "Global Reader" permissions. No user account is needed at all, as authentication/authorization is done via the registered application. Unfortunately, it is not yet possible to convert all services to the Microsoft Graph, at least not yet. In particular, the Exchange module (for reading the Exchange and compliance settings), as well as the Teams module cannot yet be replaced, as Microsoft has not yet made the necessary functions (REST API endpoints) available.

Register application in Entra ID

To register applications, you must have at least the Application Administrator role.
To do this, open the Entra ID Admin Center (https://entra.microsoft.com/) and expand the "Applications" section in the left menu bar.
Then click on "App Registrations". You will now see a list of applications already registered in your tenant.

Click on "New Registration". Give the application a name (for example, "Microsoft 365 Checker") and leave all other settings as they are. Click on "Register".

Now the application is registered and the screen should look like this:



Now open Windows Notepad (or any other word processor) and copy the "Application ID (Client)" and the "Directory ID (Tenant)" shown on this page. These will be needed later for configuring the checker.

Next, the necessary permissions must be set in the application. To do this, click on "API Permissions". By default, the Microsoft Graph has the User.Read permission of type Delegated[1].

Now click on "Add Permission" and from the list of commonly used Microsof APIs, click on "Microsoft Graph".

For the type of permissions, select "Application Permissions". You will now get a list of all possible permissions (more than 800).

Open the "Application" pane and highlight "Application.Read.All".

Scroll to the "Directory" section and highlight "Directory.Read.All".

Scroll to the "RoleManagementPolicy" section and highlight "RoleManagementPolicy.Read.Directory".

Scroll to the “RoleManagement” section and highlight “RoleManagement.Read.Exchange“.

Then click on "Add permissions" again.

Click Add permissions again, and then click APIs used by my organization. Enter "M365" in the search bar.

Select "M365 License Manager" from the list. In the Delegated Permissions pane, select LicenseManager.AccessAsUser. Click Application Permissions and enable LicensedProduct.Read.All.

Confirm with "Add permissions".

Note: The "LicenseManager" is used to read the settings for self-service purchases. Currently, the LicenseManager can only be accessed in "Delegated Mode". In the case of certificate-based login, these settings cannot be read.

Click Add permissions again, and then click APIs used by my organization. Enter "Office" in the search bar.

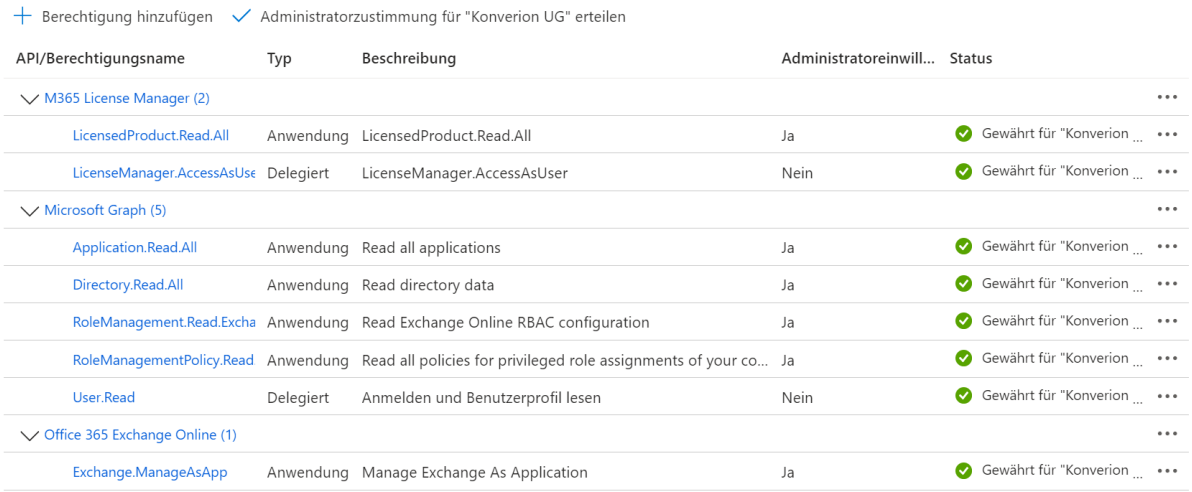
From the list, select Office 365 Exchange Online. Click on "Application Permissions" and activate "Exchange.ManageAsApp" in the "Exchange" area.

Confirm with "Add permissions".

To approve the requests, click "Grant admin consent to [your organization]" and then confirm with "Yes". The status of the permissions will change to "Granted to [your organization]".

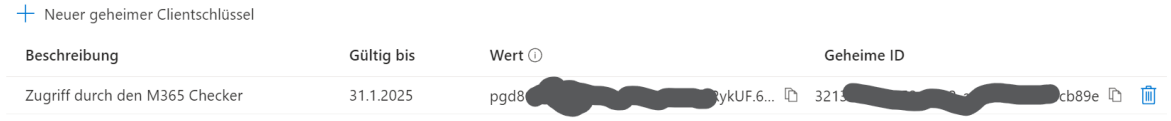
The list of configured permissions should now look like this:

[1] For the difference between the "Delegated" and "Application" permission types, see the "Permission Types" section,



Finally, access must be configured. To do this, click on "Certificates & Secrets". In the Client Secrets section, click + New Client Secret. A dialog box opens where you can specify a description of the key and a validity period. Enter "Access by the M365 Checker" as the description and select a validity period. Note: after the validity period expires, you must generate a new client key and reconfigure the checker accordingly. The period of validity cannot be extended retrospectively.

The display should now look like this:



IMPORTANT: Now copy the value (not the secret ID) into the file created above with the directory ID and the client ID.

This completes the registration of the application. You have assigned the following permissions:

Range	Right	Purpose
Microsoft Graph	Application.Read.All	Read all registered applications in Entra ID
Microsoft Graph	Directory.Read.All	Read users and groups (required to read the administrators to be able to resolve names and groups)
Microsoft Graph	RoleManagementPolicy.Read.Directory	Reading Role Assignments for Privileged Identity Management
Microsoft Graph	RoleManagement.Read.Exchange	Read Purview-Roles
M365 License Manager	LicensedProduct.Read.All	Read out settings for self-service purchases
M365 License Manager	LicenseManager.AccessAsUser	Log in to the License Manager as a user
Exchange	Exchange.ManageAsApp	Grant the application access to the Exchange and compliance configuration.

Authorization Types

When assigning permissions to access application programming interfaces (APIs) as part of application registration, a distinction is made between the types "Delegated" and "Application".

"Delegated" means that the application that wants to access data through the programming interface does so on behalf of the user, i.e. with exactly the permissions that this user already has. Delegated permissions do not assign any additional permissions, but only determine which APIs can be used to use which of a user's existing permissions. So, for example, if you grant an application the delegated permission "Mail.Read" to the Microsoft Graph, a logged-in user can also read their email from the Microsoft Graph (in addition to Outlook, Outlook on the web, etc.).

With the Application type, the application itself is granted permissions, regardless of the user logged in, or even without a logged-in user at all.So if you give an application the Mail.Read.All permission on the Microsoft Graph, that application can use the Microsoft Graph to read all emails from all users in your tenant. Regardless of who is currently using this application. Such far-reaching permissions are required, for example, for applications that are supposed to create a data backup of your files or e-mails.

Configure Microsoft 365 Checker for Graph

After starting the checker, go to "Settings" and "Graph". Enter the directory ID in the Tenat ID field, the application ID in the Client ID field, and the value you copied when you created the application secret in the Client Secret field.

Click on "Test Login".

The output should then

```
AccessToken: OK
{"@odata.context":"https://graph.microsoft.com/v1.0/$metadata#organization(displayName,city)","value":
[{"displayName":"Konverion UG","city":"Berlin"}]}
Login: OK
```

where "displayName" and "city" contain the value of your organization.

If you log in successfully, "Use graph if possible" will be activated. When you create the next report that reads Entra ID settings or self-service purchases, it uses the Microsoft Graph instead of a PowerShell module. You can disable this feature at any time until the end of March 2025 (discontinuation of the AzureAD PowerShell modules) to stop using the graph and read the settings again via PowerShell. To turn it on again, click on "Test Login" again.

Set up certificate-based login

With the certificate-based login, the checker can be used without the need for a special user account. Limitation: The optional PowerShell modules "MSCommerce" and "O365Essentials" do not support certificate-based login. The corresponding settings cannot be read out when using certificates (at least for the time being).

Both "official" and self-signed certificates can be used.

To use certificate-based login, three steps are required:

1) Create a self-signed certificate, or export the corresponding certificate files from your own PKI
2) Registering the certificate in the Entra ID app
3) Assign permissions
4) Creating a Login File

Step 1 – Create a certificate

To create a self-signed certificate, follow these steps: Open the Microsoft 365 Checker and go to Settings Cert. Click on "Create certificate".

In the window that appears, enter the file name for the certificate, the domain, and a password to encrypt the private key.
Example:

Note: The password cannot contain a "#".

Since the creation and signing of the certificate can only be done with administrator permissions, after clicking on "OK" the corresponding dialog of the User Account Control appears, requesting approval to grant increased permissions to the program "MakeCert.exe" (part of the Microsoft 365 Checker). If confirmed with "Yes", a certificate and the corresponding private key will be created.

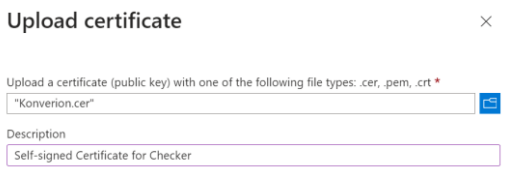
The files can be found in the directory "C:\data\office365checker\certs". If you use the file name used above, you will now find the files "ssc_Zusenberg.cer" (certificate file) and "ssc_Zusenberg.pfx" (private key) in this directory.

The certificate is also stored in your certificate store on the local machine. You can find it in the Certificate Manager (Certmgr.exe) under "My certificates". This certificate is not used and can be deleted.

Step 2 – Import certificate in the registered app

In the next step, import the certificate into the app already registered in Entra ID.

In the Entra ID admin portal, open the corresponding app (in the example: "Microsoft 365 Checker") and select "Certificates & Secrets". Here, go to the "Certificates" tab. Select "Upload Certificate". Select the certificate file you just created (in the example: "ssc_Zusenberg.cer") and enter a description.



Confirm with "Add". The added certificate appears in the list of certificates.

Step 3 – Assign permissions

If the checker authenticates itself with a certificate, this is done via the ServicePrincipal of the registered app. The ServicePrincipal must therefore have sufficient permissions to be able to read the configurations.

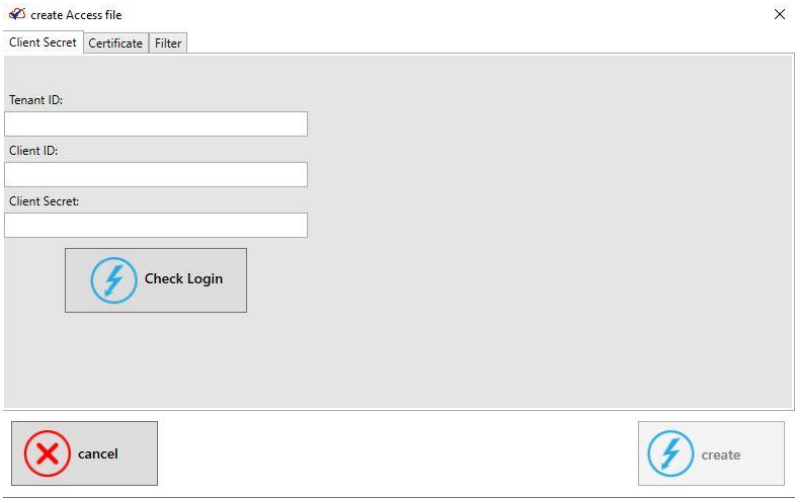
In the Entra ID Admin Center, select the “Roles and administrators” area and search for the “Global reader” role and select it. Click on “Add assignments” and enter the name of the app you have registered in the search field, select it and click on “Add”.

The ServicePrincipal of the app is now displayed in the list of assignments.

Step 4 – Create Login File

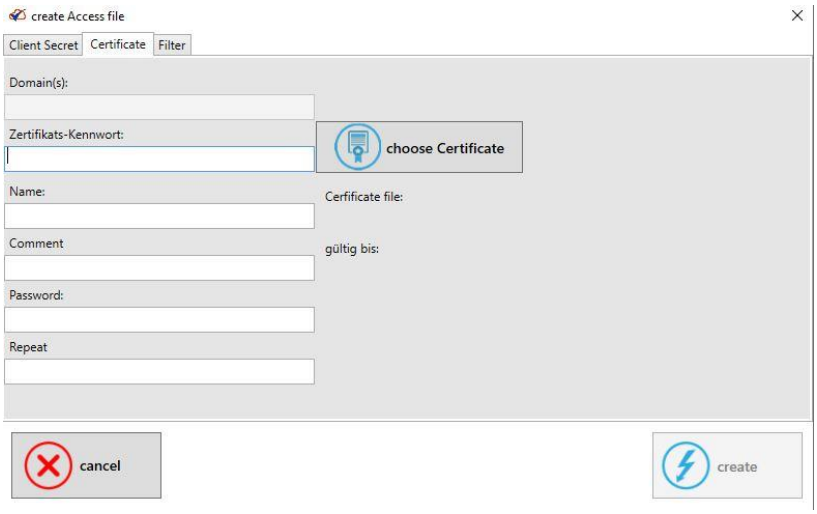
The login file is used to achieve the replacement for the "encapsulated mode". So you can make sure that the certificate can only be used by the checker. You can also set restrictions on the reports that you create. For this purpose, the password for the private key, as well as the selected restrictions, if applicable, is stored encrypted in the login file with a password to be assigned by you.

So if your works council used to use the checker in "encapsulated mode" to generate reports itself, you can now replace this with certificate-based login. To do this, enter the file with the personal key (*.pfx), the login file (*.o3s), and the password for the login file to the works council.To do this, the two files must be stored in the directory "c:\data\office365checker\certs".
Procedure:In the Microsoft 365 Checker, go to Settings and Cert. Click on "Create Login File". The following window appears:



Enter the Tenant ID, Client ID, and Client Secret as described in the "Register Application in Entra ID" section. Then click on "Test registration". If the registration is successful, the background will turn green.

Then switch to the "Certificate" file:



First, enter the password for the private key that you assigned when creating the certificate. Then click on "Select certificate" and select the created private key (*.pfx file). The path to the certificate file, the validity date, and the domain name are then read and displayed.

Now give a name for the login file to be created, a description, and a password to encrypt the login file.

If necessary, you can now set restrictions. To do this, switch to the "Filters" tab. Here you can specify that only personal data of users from a certain country (field=country), a specific company (field=CompanyName), or a specific data location (field= UsageLocation) can be read in the reports. You can also specify that only the number of administrators in the respective roles, but not their names, can be read.

Finally, click on "create".

In the directory "c:\data\office365checker\certs" a file is created with the name you specified and the extension ".o3s". This is the login file.

In the certificate settings, you will see the newly created login file in the list. You can create as many login files as you want, for example, with different filter settings.

License

In the "License" area the status of your license is displayed. Here you see the type of your license ("demo" or "general") and how long your license is still valid.

For licensed versions, it also shows for which domain(s) the Microsoft 365Checker is licensed.

Overview

The "Overview" area currently displays the number of templates and reports created.

Use deprecated features (Checker version 7.x)

Until Microsoft technically implements the announced changes, the "old" functions of the checker can continue to be used. Until the beginning of 2025, it is still possible to log in without MFA and until March 30, 2025, the Azure AD PowerShell modules can still be used.

Encapsulated mode

As shown in the section "Preparation", to use the Microsoft 365 Checker, you need a user account that has read permission for as many settings as possible in the Microsoft 365 Tenant. The easiest way to do this is through the Global Reader role. To access the AuditLogs, the account also needs the Security Read role. However, especially in larger companies, there are often concerns about providing the works council with an account with such far-reaching read rights, as this could, for example, also allow the configuration (not the content!) of managers' accounts to be viewed.

In order to provide a solution that is viable for both sides, an "encapsulated mode" has been integrated into the Microsoft 365 Checker. In this mode, the user account with the necessary authorization can only be used in conjunction with the Microsoft 365 Checker. Direct access to the Microsoft 365 tenant via the account is no longer possible. In this way, the information requirements of the works council can be satisfied on the one hand, but also the security requirements of IT on the other.

For international companies or companies with multiple works councils, the display of personal data in the reports may be restricted. This means that each works council will then only see personal data of the employees who are also represented by it.

The procedure for doing this is described in the section "Use Encapsulated Mode".

Multi-factor authentication

Starting with version 5.4, multi-factor authentication (MFA) accounts can be supported to use Microsoft 365 Checker.

In general, it should be noted that MFA and encapsulated mode are mutually exclusive, as MFA always requires an interactive login.

Therefore, since version 5.4 of the checker, you can also use the filter options independently of the encapsulated mode.

For example, when multi-factor authentication is activated, reports can be created and exported by IT to suit each works council body. Since exported reports are encrypted and provided with a hashed checksum, manipulation of the exports is not possible.

How you can use the encapsulated mode without having to forego the security of a second factor can be read in the following section.

Conditional Access policies

Since encapsulated mode and multi-factor authentication are technically mutually exclusive, conditional access policies are a good solution. This means that the interactive standard MFA procedures can be replaced by a "static" second factor. Depending on the technology used, allowed IP addresses / ranges or devices registered in Azure AD can serve as a second factor.

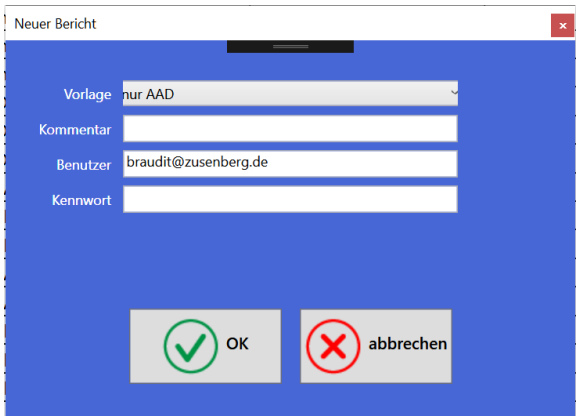
In order to be able to use the encapsulated mode with a second authentication factor, deactivate multi-factor authentication for the account that is intended for the works council controls.Then

create a policy for Conditional Access that only allows this account to log in from defined IP addresses.

For more information on how to disable MFA for individual user accounts and create Conditional Access policies, see https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa

Create a new report

To create a new report about the dialog boxes of version 7.x of the checker, hold down the left Shift key and then click on the function switch "+new". A dialog box will appear.



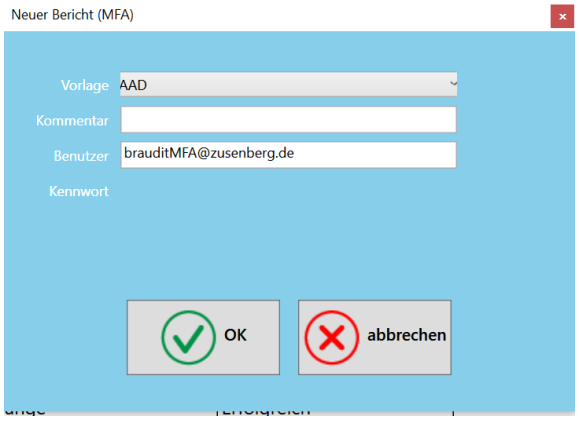
If you click on the "Template" selection field, you will be shown a list of all already defined templates that have the status "active". Select the desired template on the basis of which you want to create a report. You can already enter a comment on the report that has not yet been created. However, this can also be done after the report has been prepared.

Next, you'll need to enter a user account and the associated password that you want the Microsoft 365 Checker to use to sign in to your Microsoft 365 tenant. To successfully generate a report, the specified account must have read permissions to the services compiled in the selected template. It makes sense to use an account with the "Global Reader" authorization in Microsoft 365.

You can preset the user name in the Microsoft 365 Checker settings. The password is never stored.

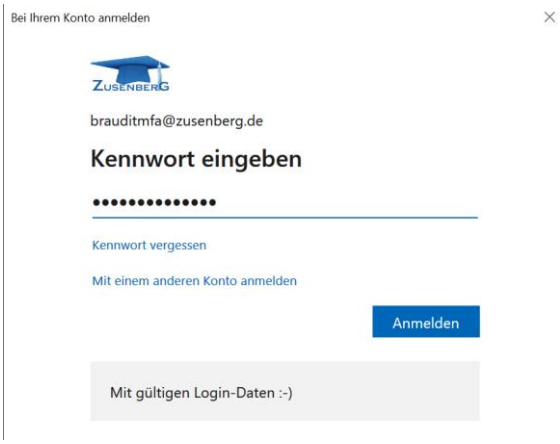
Click OK and the Microsoft 365 Checker will start generating the report.

If you use multi-factor authentication, the dialog box will look a little different:

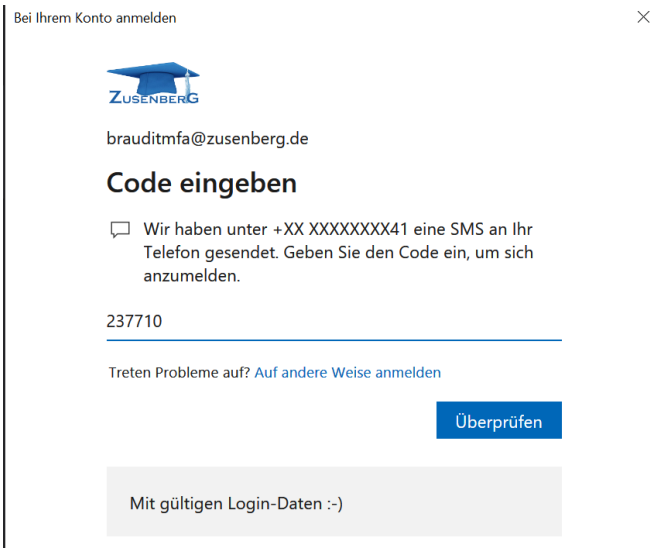


MFA always requires an interactive login, so no password can be entered in the dialog box.

If you confirm with "OK" you will receive the interactive dialog for registration



After entering the password and clicking on "Login", you will next receive the MFA prompt. Depending on the settings in the company via SMS code, authenticator app,...



After clicking on "Verify" (or confirmation by the Authenticator app), the report generation starts.

You'll see the rotating Microsoft 365 Checker logo and a "Generating report" message.

Depending on the number of configurations to be read, creating a report can take several minutes to a few hours.

When the report generation is finished, the list of existing reports is displayed again. The newly created report appears in the top row.

To view the report, select the report in the list and click View.

Use Encapsulated Mode

Note:
Since Microsoft will enforce multi-factor authentication (MFA) for all user accounts with administrative permissions from the beginning of 2025, and MFA and encapsulated mode are mutually exclusive, this mode will only be supported until the beginning of 2025.
The functionality of the encapsulated mode is replaced by the certificate-based login, which is available from version 8 of the checker.

With the encapsulated mode, the use of the user account, which is equipped with the read permissions for the configuration of the tenant, is limited to the Microsoft 365 Checker.

Normally, the works council is given an account with the "Global Reader" authorization to exercise its control rights (example: braudit@zusenberg.de). This account can also be used to sign in to the various Microsoft 365 admin centers, so that access to the configuration of executive accounts would also be possible.

In encapsulated mode, this account is set up in the same way, but the works council no longer receives the password for this account, but an encrypted file, as well as an encryption password with which the Microsoft 365 Checker can decrypt the file.

For technical reasons, this approach only works with accounts that do not have multi-factor authentication (MFA) enabled. MFA always requires an interactive login.

The file itself (Office365Checker.o3c) is encrypted and contains the hash value of the username and the corresponding password. Even if this file fell into "wrong hands" and could be decrypted, the account would not be compromised because the username is only stored as a hash value.

In encapsulated mode, the works council therefore needs the following for the use of the Microsoft 365 Checker:

- the name of the user account,
- the file "Office365Checker.o3c", and
- the password to use this file.

This means that you can no longer sign in directly to Microsoft 365 with this account.

To use this mode, do the following:

1. IT creates the user account (in the example: braudit@zuenberg.de with the password "!streng9Geheim")
2. With the help of the Microsoft 365 Checker, IT creates the file "Office365Checker.o3c" with the encryption password "#IT.encrypted!"
3. The works council receives:
    a. the username "braudit@zusenberg.de"
    b. the file "Office365Checker.o3c"
    c. the encryption password "#IT.encrypted!"
4. The works council saves the file in the directory "c:\data\Office365Checker".
5. When creating a new report, the Microsoft 365 Checker recognizes the file and prompts for the username and encryption password.

Ideally, not everything in one email!

6. The encryption password is used to decrypt the file and read the user password "!streng9Geheim". In addition, the program checks whether the username entered corresponds to the username stored as a hash value in the file.
7. The Microsoft 365 Checker signs in to Microsoft 365 with the account braudit@zuenberg.de and password "!streng9Geheim" and creates the desired reports.

Limit the results

You can restrict the display of personal data (name, email address,..) in the reports. This applies in particular to the Exchange Litigation Hold and Journal functionalities, as these are explicitly applied to specific users. This is useful, for example, in order to include only the data of German users in the reports in an international company, since only they are represented by the works council. Even if several German companies are combined in a common tenant but have different works councils, you can achieve by restricting that each works council only sees the data of the employees it represents.

These restrictions can be based on the CompanyName, Country or Country, or UsageLocation fields.

Example: In the tenant of an international company, all users have the "Country or Region" attribute filled in with the country code corresponding to the employee's location. For all those resident in Germany, this means with "DE". If you now create an "Office365Checker.o3c" file with the restriction "Country=DE", only usernames of German employees will be displayed in the reports under the items "Journal" or "Preservation of evidence". For all others, "anonymized" appears:

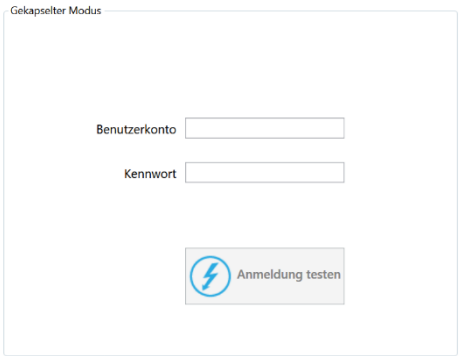
So the first user is not based in Germany, but "Julia Huber" is.

The email address of the administrator who has made the corresponding configuration will be displayed in any case in order to be able to ask questions if necessary.

Furthermore, you can specify that only the number of administrators assigned to the respective role is read out for the authorizations, but no longer the specific names.

Creating the "Office365Checker.o3c" File

To create the Office365Checker.locked file, go to the Settings pane.



In the "Encapsulated mode" area, enter the user name (in the example: braudit@zusenberg.de" and the corresponding password (in the example: "!streng9Geheim"). Click on the "Test Login" toggle. The Microsoft 365 Checker will then test the sign-in to your Microsoft 365 tenant with the information provided. If the login was successful, an input field for the encryption password appears and the switch changes to "Create file".

If you have selected the "Limit results" checkbox, the set restrictions are encrypted with in the "Office365Checker.o3c" file, and therefore cannot be changed by the subsequent user.

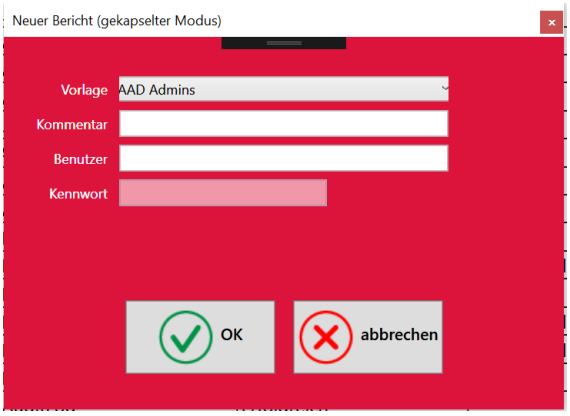
Enter the encryption password (in the example: "#IT.encrypted!") and click on "Create file". Note: the encryption password will be displayed in plain text until the file is saved. A dialog box will appear where you can choose where to save the file.

Now you can make the saved file available to the works council. This stores them in the folder "C:\data\Office365Checker" on the computer on which the Microsoft 365 Checker is to run.

Also inform the works council of the user name and encryption password.

Create reports in encapsulated mode

Click the Reports section, hold down the left Shift key, and then click the +New switch.



If the file "Office365Checker.o3c" exists in the directory "C:\data\Office365Checker", a special dialog box for generating reports in encapsulated mode is displayed.

Select the template for the desired report.

Then enter the user name (in the example: "braudit@zusenberg.de") and the encryption password (in the example: "#IT.encrypted!").

Click OK and the report will be generated.

Secure the encapsulated mode with a second authentication factor

Because multi-factor authentication always requires interactive login, user accounts that have MFA enabled cannot be used for encapsulated mode.

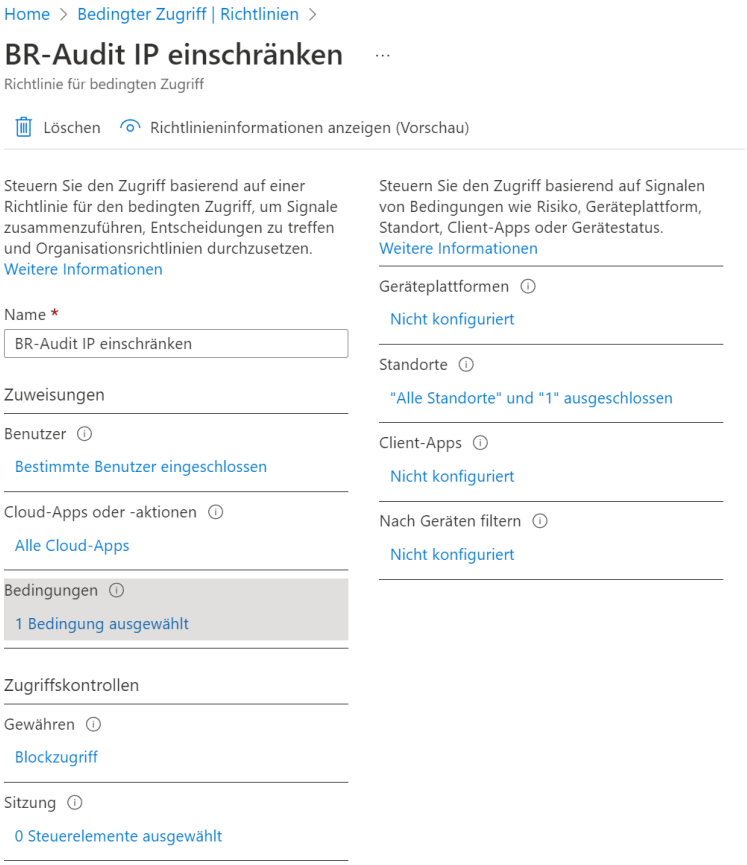
In order to be able to make use of the increased security of a second authentication factor even in encapsulated mode, the use of "Conditional Access Policies" is recommended. This means that you can require a certain IP address/range as a second factor, for example, or a registered PC (requires the use of Microsoft Intune).

To do this, proceed as follows (example of restriction to a specific IP address):Create the desired user account (in the example, "braudit-ip@zusenberg.de") and assign it the roles of "Global Reader " and "Security Reader".

Make sure that MFA is not enabled for this account (you may need to add an exception to your Conditional Access policies). In Azure Active Directory, create a named location in the Conditional Access pane. Here you can specify the IP address or IP range from which the account can log in. For example, you can ensure that login is only possible from the company network.

Next, create a new Conditional Access policy. As a user, enter the BR control account. Under "Cloud Apps and Actions," select "All Cloud Apps." Under "Condition", enter "All locations" under "Locations" under "Include", and under "Exclude" enter the location you have just created. Under "Grant" enter "Block access". Toggle "Enable Policy" to "On" (or "Report Only" if you want to test it first).

The guideline should now look something like this:



Click Save.

If you want to test the policy, click on the corresponding policy and select "WhatIf" from the top menu bar. Here you can test when and how the policy affects by specifying different usernames/IP addresses.

After the new policy is enabled, the Microsoft 365 Checker can only be used with the registered user account from the specified IP address.

Troubleshooting

The most common problem when using the Microsoft 365Checker occurs when the installation was not performed with an account that has administrative rights on the local PC.

This may manifests itself by the Microsoft 365 Checker quitting right after it starts.

If this is the case, check whether there is a subdirectory "PS" in the directory "c:\data\Office365Checker", which in turn contains the subdirectories "AzureAD", "ExchangeOnlineManagement" and "MicrosoftTeams".

If this is not the case, start the PowerShell console ISE as administrator.

Run the command
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser -Force

Next, open the file open the file “c:\data\Office365Checker\PS\installNuget.ps1” and run it to install the NuGet Package Provider. This is necessary to copy the required PowerShell modules from Microsofts PowerShell Gallery.

Next, open the file "c:\data\Office365Checker\copyModules.ps1" and run it. This will install the required PowerShell modules.

If you encounter other problems, open the "log.txt" file with a text editor. In it, all error messages of the Microsoft 365Checker are recorded. This will allow you to determine, among other things, if the account you used to read the configuration does not have sufficient permissions.

If you are unable to solve any problems yourself, please contact us at support@konverion.de. We will contact you as soon as possible.

Appendix: Readable Settings

Unified Audit Log

The events of the following categories are read out from the Unified Audit Log:

eDiscovery
Advanced eDiscovery
Settings for Anonymizing Usage Reports
User Added to a Role (Made an Administrator)User Removed from a Role (Admin Rights Revoked)
WorkplaceAnalytics

To keep the reports clear, the actions taken for eDiscovery, Advanced eDiscovery, and Workplace Analytics are grouped into categories and the total number of actions per category is recorded. The explanations of the meaning of "Operations" can be found here: https://docs.microsoft.com/de-de/microsoft-365/compliance/search-for-ediscovery-activities-in-the-audit-log?view=o365-worldwide The changes to the settings for anonymizing the usage reports, as well as for adding and removing the administrator role to users and groups are listed individually.

Example usage reports

Name **Berichte anonymisieren**

Operation	Count	Details
UpdatedCFRPrivacySettings	1	11.02.2022 22:44:30 joergsc@zusenberg.de # {Name:PrivacyEnabled,OldValue:False,NewValue:True}]
UpdatedCFRPrivacySettings	1	11.02.2022 08:40:13 joergsc@zusenberg.de # {Name:PrivacyEnabled,OldValue:True,NewValue:False}]

Meaning:On 11.02.2022 at 08:40 a.m., the anonymization of the usage reports was switched off by the user "joergsc@zusenberg.de", on the same day at 10:44 p.m. it was turned on again.

Example of assigning administrator permissions:

Name **Role Membership added**

Operation	Count	Details
Add member to role.	1	11.02.2022 11:18:09 joergsc@zusenberg.de # NewValue:User Account Administrator, : brauditttest@zusenberg.de

On 11.02.2022 at 11:18 a.m., the user brauditttest@zusenberg.de was assigned the role of "User Account Administrator" by the user joergsc@zusenberg.de.

Example revocation of administrator permissions:

Name **Role Membership removed**

Operation	Count	Details
Remove member from role.	1	11.02.2022 11:14:30 joergsc@zusenberg.de # ,OldValue:Global Reader},{Name : brauditttest@zusenberg.de

On 11.02.2022 at 11:14 a.m., the user brauditttest@zusenberg.de the role "Global Reader" was revoked by user joergsc@zusenberg.de.

Azure Active Directory

Info

Name of the tenantAddress (street, zip code, city)CountryPhonePrivacy ContactURLAnnumber of users

AAD Rollers

All roles with:NameDescriptionRole holder with surname, first name and email address

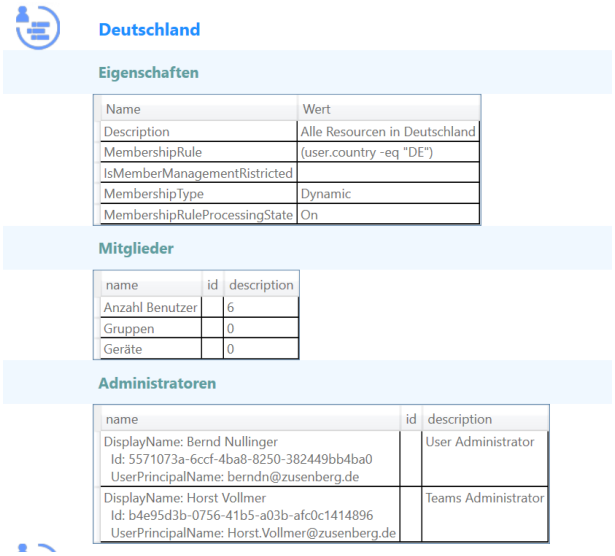
AAD Apps

All registered apps with:NameDescriptionOwnerPermissionsNote: Application permissions to the Microsoft Graph API are highlighted (an exclamation mark appears under the wrench icon for the app. The permissions indicate whether they are delegated or application permissions.

AAD Administrative Units

With administrative units in Azure Active Directory, administrator roles can be set for individual areas (users, groups, devices).
For a description, see https://learn.microsoft.com/de-de/azure/active-directory/roles/administrative-units

For example,



Deutschland

Eigenschaften

Name	Wert
Description	Alle Resourcen in Deutschland
MembershipRule	(user.country -eq "DE")
IsMemberManagementRistricted	
MembershipType	Dynamic
MembershipRuleProcessingState	On

Mitglieder

name	id	description
Anzahl Benutzer		6
Gruppen		0
Geräte		0

Administratoren

name	id	description
DisplayName: Bernd Nullinger Id: 5571073a-6ccf-4ba8-8250-382449bb4ba0 UserPrincipalName: berndn@zusenberg.de		User Administrator
DisplayName: Horst Vollmer Id: b4e95d3b-0756-41b5-a03b-afc0c1414896 UserPrincipalName: Horst.Vollmer@zusenberg.de		Teams Administrator

for dynamic membership rules, the MembershipRule attribute contains the rule for creating it. In the example, the "Germany" administrative unit contains all users for which the country attribute is set to "DE". If users, groups and devices are assigned manually, all attributes except the description are empty.

The Members table shows the total number of associated users, groups, and devices.

The Administrators table lists the administrators and roles associated with this administrative unit. The names of the administrators will only be displayed if you have not selected "Show only number of administrators" in the settings.
In the future, it will also be possible to link policies to prevent data loss to administrative units. This functionality is currently in preview.

Privileged Identity Management

If there are licenses in tenant E5, "Privileged Identity Management (PIM)" can be used for a variety of roles. This makes it possible to ensure that administrators do not have standing authorizations, but authorizations are only granted when they are specifically needed. This means that administrators are no longer directly assigned to an AzureAD role, but managed via PIM. There are two options for assigning a role: "active" or "eligible".
If an assignment is "active", it does not need to be applied for separately. So it corresponds to the direct assignment to a role. However, PIM can be used to set the start and end dates of the assignment, so that the permissions are only available for a certain period of time. If an assignment is "eligible", the administrator must apply for permission via a website. Approval can be automatic or granted by specified persons.

If the "AzureADPreview" PowerShell module is installed, the Microsoft 365 Checker can read the PIM roles and assignments.

All available roles will then be listed. Example:

Teams Devices Administrator

If there are assignments for a role, they are displayed below the role. In the example below, the checker was set to "Show number of administrators only", so the names of the authorized admins are not displayed here.

Teams Administrator

Eigenschaften

Name	Wert
AssignmentState	Eligible
MemberType	Direct
StartDate	07.05.2023 15:24:29
EndDate	

Member

displayName	givenName	surname	email
Anzahl		1	

Eigenschaften

Name	Wert
AssignmentState	Eligible
MemberType	Direct
StartDate	13.06.2023 07:46:31
EndDate	

Member

displayName	givenName	surname	email
Anzahl		1	

Licenses

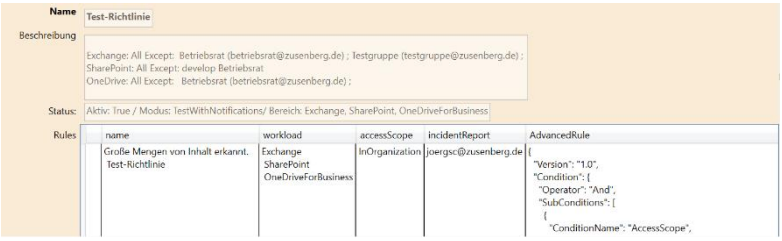
All available licenses with:Number of available licensesNumber of assigned licenses

Microsoft 365 Security & Compliance

Data Loss Prevention DLP (Verhindern von Datenverlust)

All DLP rules with:NameDescriptionStatusModeAffected areas (Exchange, SharePoint, OneDrive for Business, Teams)
Exclusions from affected areasAdvanced rules – the specific settings of the rules

Example:



This DLP rule affects the areas (workloads) Exchange, SharePoint and OneDrive.
Exchange excludes all users who belong to the betriebsrat@zusenberg.de or testgruppe@zusenberg.de groups. SharePoint excludes the Develop and Works Council sites, and OneDrive excludes all members of the betriebsrat@zusenberg.de group.

Because the display of the "AdvancedRules" takes up a lot of space and can thus lengthen a report considerably, the "AdvancedRules" are not displayed in the filtered view.

Activity notifications

All activity notifications with:NameDescriptionOperationMessage to

Security Notifications

All security notifications with:NameDescriptionOperationMessage to

AuditLog Retention Policies

All retention policies with:NameDescription
StatusOperationsData Types
UserIds

Retention

All retention policies with:NameDescription
Status Mode
WorkloadCreation DateCreator
All rules with name, query, type, retention days, and action

Communication Compliance

All communication compliance policies with:NameDescription
ModeStatusAll defined rules in JSON format

Insider Risiko Management

All policies with:NameDescriptionStatusTypeScenarioWorkloadCreatorLast ModifiedExchange ObjectID

Content Search

All Content Searches With:NameDescriptionSearch ByCreated ByLast ModifiedIncluded and Excluded Areas

eDiscovery

Note: To read the eDiscoveries, the role "Global Reader" is not sufficient!

NameDescriptionStatus
Last ModifiedCase Admin

Advanced eDiscovery

Note: To read the Advanced eDiscoveries, the role "Global Reader" is not sufficient!

NameDescriptionStatusLast ModifiedCase-Admin

Data Subject Requests

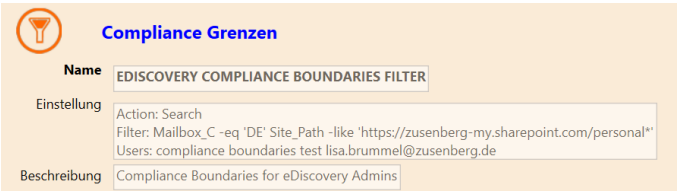
Note: To read the Data Subject Requests, the role "Global Reader" is not sufficient!

NameDescriptionStatusCreated onLast modified byEditor

Compliance Boundaries

All compliance boundaries set up with the associated search filters and users/groups

For example,



the compliance boundary applies to all users from the compliance boundaries test group, as well as to lisa.brummel@zusenberg.de.

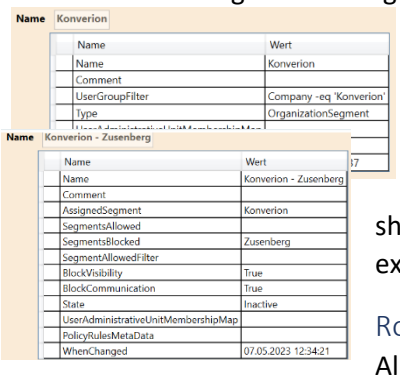
Even if they have been assigned compliance roles in the compliance center, users cannot search the mailboxes of users that have the country code "DE" entered (filter: Mailbox_C – eq 'DE' / Note: in Exchange, the country attribute has the abbreviation 'C', not 'country' as in AzureAD!) and they cannot search OneDrive folders at all (filter: Site_Path -like 'https:/ zusenberg-my.sharepoint.com/personal*').

Information barriers

Via "Information barriers, communication between defined user groups can be prevented / only affects chat and shares, e-mails cannot be prevented this way).

To do this, you first define the corresponding segments, and then the guidelines for which segments should be isolated from which. Example segments:

The "Konverion" segment is assigned to all users for whom the company name "Konverion" is entered.



Example policy:

The policy is associated with the Konverion segment and prevents members of the Konverion segment from seeing, chatting, or sharing files with those from the Zusenberg segment. However, the example policy is not enabled (State: Inactive).

Roles

All Microsoft 365 roles with:NameDescriptionMembers (display name, last name, first name, email address)

Exchange

Info

Name der OrganisationStandard-RegionSharePoint URLRead Tracking LockBoxAuditing

Transport

All transport rules with:NameDescriptionStatusLast modified

Data Loss Prevention

All DLP rules with:NameDescriptionStatusMode

Journal

All journal rules with:NameMonitored Mailbox / DistributorJournal Recipient ScopeModeLast modified

eDiscovery

All Exchange eDiscoveries with:NameDescriptionSource
Last Executed ByLast Run

Retention

All defined retention policies with:NameDescription
Type
WorkloadDate createdCreatorName of associated rules
Retention DurationRetention Type QueryStart
Time

Teams

Message Policies

All message policies with: name, description, and the following parameters:

Parameter	Meaning
AllowUrlPreviews	Preview web pages when a URL has been pasted into a chatPossible values: true / false
AllowOwnerDeleteMessage	Owners of a team can delete all messages on the team Possible values: true / false
AllowUserEditMessage	Users can change their own messages Possible values: true / false
AllowUserDeleteMessage	Users can delete their own messages Possible values: true / false
AllowUserChat	Determine whether users can compose chats and channel messages. Possible values: true / false
AllowRemoveUser	Users can remove other users from chats Possible values: true / false
AllowUserTranslation	Users can have messages automatically translated Possible values: true / false
ReadReceiptsEnabledType	Message read receipt settings Possible values: UserPreferenceEach user can choose the reading receipt setting Everyone Read receipt for everyone None Read receipt for everyone off
AudioMessageEnabledType	Determines whether users can send voice messages. Possible values ChatsAndChannels Voice messages can be created in chats and channel messages ChatsOnly Voice messages can only be created in chats Disabled Unable to create voice messages
AllowUserDeleteChat	Users can delete chat histories from their view Possible values: true / false
AllowGiphys	Giphys can be inserted into messages Possible values: true / false
AllowMemes	Memes can be inserted into messages Possible values: true / false
AllowStickers	Stickers can be inserted into messages Possible values: true / false

AllowFluidCollaborate	Microsoft Fluid components can be integrated into messages Possible values: true / false
AllowPriorityMessages	Allow priority messages Possible values: true / false
AllowSmartReply	Suggested responses appear in chats Possible values: true / false
AllowSmartCompose	Text suggestions for chat messages appear Possible values: true / false
ChannelsInChatListEnabledType	On mobile devices, preferred channels appear above all others DisabledUserOverride Off, can be changed by the user EnabledUserOverride On, can be changed by the user
ChatPermissionRole	Determines the user's role in attended chats. Possible values: Full the user can supervise chats. Supervisors have the ability to initiate and invite chats with any user within the environment. Limited Users can initiate conversations with users with full and limited permissions, but not with limited users. Restricted Users can only chat with users with full permission
AllowFullChatPermissionUserToDeleteAnyMessage	Users with the ChatPermissionRole "Full" can delete all messages Possible values: true / false
AllowVideoMessages	Video messages can be created and sent Possible values: true/ false
AllowCommunicationComplianceEndUserReporting	Users can report inappropriate messages in Chat. Only available in conjunction with E 5 licenses and "Communication Compliance" Possible values: true / false

The Global message policy is the default policy for all users.
If not all listed parameters appear in your report, update the PowerShell module "MicrosoftTeams" to the latest version via the "Settings / PS" area.

Meeting Policies

All meeting policies with: name, description, and the following parameters:

Parameter	Meaning
AllowChannelMeetingScheduling	Channel meetings can be scheduledPossible values: true / false

AllowMeetNow	Ad-hoc meetings can be heldPossible values: true / false
AllowPrivateMeetNow	Private ad-hoc meetings can be heldPossible values: true / false
MeetingChatEnabledType	Specifies whether users can chat in meetings. Mögliche Werte: Disabled, Enabled, EnabledExceptAnonymous
LiveCaptionsEnabledType	Enable live captions in meetings Possible values: Disabled / DisabledUserOverride
AllowIPVideo	Users can use video in meetings. Possible values: true / false
AllowAnonymousUsersToDialOut	Anonymous users can make landline calls. Possible values: true / false
AllowAnonymousUsersToStartMeeting	Anonymous users can start meetings. Possible values: true / false
AllowPrivateMeetingScheduling	Users can schedule private meetings. Possible values: true / false
AutoAdmittedUsers	Determines who automatically bypasses the meeting lobby Mögliche Werte: EveryoneInCompany, EveryoneInSameAndFederatedCompany, Everyone, OrganizerOnly, EveryoneInCompanyExcludingGuests, InvitedUsers
AllowCloudRecording	Allows you to record meetings Possible values: true / false
AllowOutlookAddIn	Determines whether users can schedule meetings from the Outlook client. Possible values: true / false
AllowPowerPointSharing	Allow sharing PowerPoint presentations in meetings. Possible values: true / false
AllowParticipantGiveRequestControl	Users can request control over screen sharing in meetings. Possible values: true / false
AllowExternalParticipantGiveRequestControl	External users can request control over screen sharing in meetings. Possible values: true / false
AllowSharedNotes	Allow shared meeting notes Possible values: true / false
AllowWhiteboard	Allow whiteboard in meetings. Possible values: true / false
AllowTranscription	Allow transcription of meetings. Possible values: true / false
AllowEngagementReport	Attendance lists are created for meetings that the organizer can download Possible values: Enabled / Disabled
ScreenSharingMode	Determine how screen content can be shared in meetings. Possible values: EntireScreen / SingleApplication

AllowPSTNUsersToBypassLobby	Users who dial into a meeting by phone can bypass the waiting room. Possible values: true / false
AllowOrganizersToOverrideLobbySettings	Meeting organizers can change the Waiting Room settings Possible values: true / false
RecordingStorageMode	Where to store meeting recordings OneDriveForBusiness
AllowCloudRecordingForCalls	Allows you to record 1:1 meetings Possible values: true / false
VideoFiltersMode	Allowed wallpapersPossible values: NoFilters, BlurOnly, BlurAndDefaultBackgrounds, AllFilters
AllowMeetingReactions	Allow reactions in meetings Possible values: true / false
AllowMeetingRegistration	Allow webinars Possible values: true / false
MeetingRecordingExpirationDays	Retention period of recordings in days
AllowNDIStreaming	Audio and video of meetings can be streamed via NDI Possible values: true / false
SpeakerAttributionMode	Save Speaker Names to Recordings Disabled, EnabledUserOverride
AllowBreakoutRooms	Enabling group rooms Possible values: true / false
AllowMeetingCoach	Allow speaker coach in meetings. Possible values: true / false
ChannelRecordingDownload	Recordings of channel meetings can be downloaded. Possible values: Allow/Block
AllowTasksFromTranscript	Tasks can be created from the transcription. Possible values: Enabled / Disabled
InfoShownInReportMode	Determines what information is available in attendance reports. Possible values: identityOnlyOnly the names of the participants are captured FullInformation The names of the participants, as well as the exact times of participation (entry / exit) are recorded
QnAEngagementMode	Allow question and answer tool in meetings. Possible values: Enabled / Disabled
AllowAvatarsInGallery	Allow avatars in the gallery view: Possible values: true / false
AllowWatermarkForScreenSharing	Allow watermarks in shared screen content (Teams Premium only) Possible values: true / false
AllowWatermarkForCameraVideo	Allow watermark for user video (Teams Premium only) Possible values: true / false

IPAudioMode	IP Audio Mode EnabledOutgoingIncoming
IPVideoMode	IP Video Mode EnabledOutgoingIncoming
ExplicitRecordingConsent	Meeting recording requires the consent of all participants Possible values: Enabled / Disabled
AudibleRecordingNotification	An audible announcement is made when a meeting is recorded Possible values: PstnOnly
CopyRestriction	Determines whether users in a chat meeting can copy messages from the clipboard. Possible values: true / false
RoomPeopleNameUserOverride	There is no description for this parameter yet. Possible values: true / false
CopilotWithoutTranscript	This parameter is no longer used
Copilot	Specifies whether Copilot works with a persistent or non-persistent transcript. Possible values: EnabledWithTranscript
AutomaticallyStartCopilot	Copilot in Teams starts automatically Possible values; enabled / disabled
VoiceIsolation	Specifies whether users can use AI-powered noise cancellation in meetings. Possible values: enabled / disabled
EnrollUserOverride	Determines whether users can register their voice profiles in the Teams client. Possible values: enabled / disabled (default)
RoomAttributeSeOverride	Determines whether users in Teams Rooms can be recognized by their voice. Possible values: **Off** Teams-Room users are not recognized. The voice profiles of the users are not used. **Attribute** If users have registered their voice profile, this is used to identify and name the users. **Distinguish** If users have registered their voice profile, it will be used to identify the users, but the users will only be tagged with speaker(s).

Webinar Guidelines

Parameter	Meaning
AllowWebinars	Users can create webinars Possible values:Enabled / Disabled
Description	Description of the policy
EventAccessType	Determines who can register for webinars. Possible values: Everyone – anyone can register, including guests and external parties EveryoneInCompanyExcludingGuest: only users of their own tenants can register
AllowTownHalls	No impact at the moment Possible values:Enabled / Disabled
AllowEmailEditing	No impact at the moment Possible values:Enabled / Disabled

Live Event Policies

All live event policies with name, description, and the following parameters:

Parameter	Meaning
AllowBroadcastScheduling	Users can schedule live events Possible values: true / false
AllowBroadcastTranscription	Live events can be transcribed. Possible values: true / false
BroadcastAttendeeVisibilityMode	Determines who can participate in live events. Mögliche Werte:Everyone, EveryoneInCompany. InvitedUsersInCompany, EveryoneInCompanyAndExternal, InvitedUsersInCompanyAndExternal
BroadcastRecordingMode	Live Event Recording ModePossible values: AlwaysEnabled, AlwaysDisabled, UserOverride

AI Guidelines

The AI policies will turn on or off users' ability to register their voice profile for intelligent noise cancellation and their face profile for person recognition in Teams rooms.

Parameter	Meaning
Identity	Policy Name
EnrollVoice	Users can register voice profile Possible values: enabled / disabled
EnrollFace	Users can register facial profile Possible values: enabled / disabled

App Permissions

All app permission policies with names and the following parameters:

Parameter	Meaning
DefaultCatalogApps	List der Microsoft Apps

GlobalCatalogApps	List of third-party apps
PrivateCatalogApps	List of custom apps
DefaultCatalogAppsType	Setting whether the list of Microsoft apps contains the allowed or blocked apps Possible values: BlockedAppList, AllowedAppList
GlobalCatalogAppsType	Setting whether the list of third-party apps contains the allowed or blocked apps Possible values: BlockedAppList, AllowedAppList
PrivateCatalogAppsType	Setting whether the list of self-created apps contains the allowed or blocked apps Possible values: BlockedAppList, AllowedAppList

Compliance Records Guidelines

All Compliance Guidelines Recording Conversations with:NameDescription StatusRegistered Application

Microsoft Viva

Viva Insights

All roles defined for Viva, as well as their owners.

Note: Only members of the Analyst role can create their own queries and evaluations beyond the predefined analyses of Viva Insights. Members of this role group will therefore have access to all the functionalities of the former Workplace Analytics!

Self-service shopping

Here you can see all the products for which Microsoft enables self-service purchases:

	Service	Setting	ProductID
	Power Automate per user	Enabled	CFQ7TTC0LH3L
	Power Apps per user	Enabled	CFQ7TTC0LH2H
	Power BI Pro	Enabled	CFQ7TTC0H9MP
	Project Plan 1	Enabled	CFQ7TTC0HDB1
	Project Plan 3	Enabled	CFQ7TTC0HDB0
	Visio Plan 1	Enabled	CFQ7TTC0HD33
	Visio Plan 2	Enabled	CFQ7TTC0HD32
	Power Automate RPA	Enabled	CFQ7TTC0KXG6
	Power BI Premium per user	Enabled	CFQ7TTC0H6RP
	Windows 365 Enterprise	Enabled	CFQ7TTC0HHS9
	Windows 365 Business	Enabled	CFQ7TTC0J203
	Windows 365 Business with Windows Hybrid Benefit	Enabled	CFQ7TTC0HX99
	Viva Learning	Enabled	CFQ7TTC0HVZG
	Dynamics 365 Marketing	Enabled	CFQ7TTC0LH3N
	Dynamics 365 Marketing Attach	Enabled	CFQ7TTC0LHWP
	Microsoft 365 F3	Enabled	CFQ7TTC0LH05
	Dynamics 365 Marketing Additional Application	Enabled	CFQ7TTC0LHVK
	Dynamics 365 Marketing Additional Non-Prod Application	Enabled	CFQ7TTC0LHWM
	Viva Goals	Enabled	CFQ7TTC0PW0V
	Power Automate Per User with Attended RPA Plan	Enabled	CFQ7TTC0LSGZ
	Teams Exploratory	Enabled	CFQ7TTC0J1FV
	Python On Excel	Enabled	CFQ7TTC0S3X1
	Teams Premium	Enabled	CFQ7TTC0RM8K
	Microsoft Purview Discovery	Enabled	CFQ7TTC0N8SL
	Microsoft ClipChamp	Enabled	CFQ7TTC0N8SS

The possible values under "Settings" are:

Setting	**Effect**
Enabled	Users can make self-service purchases and register for trials
OnlyTrialsWithoutPaymentMethod	Users cannot make self-service purchases, but they can purchase free trials of products that do not require them to provide a payment method. After the trial ends, a user will not be able to purchase the paid version of the product.
Disabled	Users cannot make self-service purchases and register for trials

Organization Settings

General settings

Tenant Primary NameNotification LanguageTechnical ContactPrivacy ContactPrivacy ContactPrivacy URL

Data storage location

Die Datenspeicherorte (data-at-rest location) fürExchangeSharePointTeams ExchangeOnlineProtectionViva Topics
Viva ConnectionsOneDrive for Business

Indication whether Multi-Geo is used (true/false)

Lockbox

Indication of whether Customer Lockbox is enabled (true / false)

Introductory Assessment

Parameter	Meaning
ProductivityScoreOptedIn	Specifies whether all users and groups are included in the calculation of the productivity score Possible values: true / false
OperationUserPuid	
OperationTime	

Graph Data Connect

Parameter	Meaning
ServiceEnabled	Service activated? Possible values: true / false
TenantLockBoxApproverGroup	Default approval group that needs to approve access
TenantLockBoxDataAccessPolicyType	Policy type for Graph Data Connect access
IsOdspEnabled	Access to OneDrive and SharePoint allowed? Possible values: true/ false
IsCrossTenantDataMovementEnabled	Data transfer to other tenants allowed? Possible values: true/ false
IsvivaInsightsEnabled	Viva Insights turned on? Does not refer to Viva Personal Insights, but the former Workplace AnalyticsPossible values: true/ false

Reports

"Reports" refers to the usage reports in the various admin centers.

Parameter	Meaning
GraphApiEnabled	Access via Graph API allowed? Possible values: true/ false
PowerBiEnabled	Make reporting data available to Power BI? Possible values: true/ false
PrivacyEnabled	Use pseudonymous identifiers in all reports? Possible values: true/ false
Region	Region where the data is processed
TenantId	GUID of the Tenants

PBIStatusUpdateDate	The date and time when the usage data was last transferred to Power BI
PBIStatus	PowerBI Processing StatusPossible values: completed

Bookings

Parameter	Meaning
Enabled	Turn bookings on/off for the entire tenantPossible values: true/ false
SocialSharingRestricted	The "Connect to Facebook" toggle will be removed
BookingsExposureOfStaffDetailsRestricted	No employee data is sent in communication with customers Possible values: true/ false
StaffMembershipApprovalRequired	Users must request to share their calendar in Bookings and be listed as a staff member in Bookings Possible values: true/ false
BookingsSmsMicrosoftEnabled	Microsoft can send SMS to customers to confirm appointments Possible values: true/ false
BookingsSearchEngineIndexEnabled	Prevents Bookings' booking pages from appearing in Bing or Google search results Possible values: true/ false
BookingsNamingPolicyEnabled	Enforce naming conventions for the Bookings calendarsPossible values: true/ false
Other parameters	Explanations of the other parameters can be found under https://learn.microsoft.com/de-de/microsoft-365/bookings/turn-bookings-on-or-off?view=o365-worldwide

Forms

Parameter	Meaning
ExternalCollaborationEnabled	Enable collaboration with external parties Possible values: true/fasle
ExternalSendFormEnabled	A link to the form can be sent to external parties to collect responses Possible values: true/fasle
ExternalShareCollaborationEnabled	Form can be edited together with external parties Possible values: true/false
ExternalShareTemplateEnabled	Form els template can be shared with external parties Possible values: true/false
ExternalShareResultEnabled	Results summary of a form can be shared with external parties Possible values: true/false
RecordIdentityByDefaultEnabled	Capture names by default Possible values: true/false
BingImageSearchEnabled	Allow you to add images from Bing and YouTube videos in Forms
InOrgFormsPhishingScanEnabled	Enable internal protection against phishing Possible values: true/false
InOrgSurveyIncentiveEnabled	Currently not in use

Cortana

Parameter	Meaning
Enabled	Allow Cortana on Windows 10 and the Cortana app on iOS and Android to access Microsoft-hosted data on behalf of people in your organization. Cortana uses this data to help employees in your organization stay in the loop and gain insights about their meetings, documents, and relationships. Possible values: true/false

MyAnalytics

These settings apply to all users.

Parameter	Meaning
EnableInsightsDashboard	Das Viva Dashboard erlauben (Viva Insights (office.com)) Possible values: true/false
EnableWeeklyDigest	Send weekly email summary to user (Can be overridden by user) Possible values: true/false
EnableInsightsOutlookAddIn	Allow the Insights add-in in OutlookPossible values: true/false

Item Insights

Parameter	Meaning
AllowItemInsights	Turn on item insights for all users (If item insights are generally allowed, they can be turned off by any user in their privacy settings) Possible values: true/false
DisabledForGroup	Item insights are turned off for certain groups of users. Possible values: true/false
DisabledForGroupID	If item insights are turned off for specific groups, here are the IDs of the groups

Meeting insights

Parameter	Meaning
AllowMeetingInsights	Meeting Insights are turned on for all users in the tenant Possible values: true/false

Licenses

The content is the same as in the Licenses section in Azure Active Directory, but the understandable names of the licenses are also displayed here.

For example, not only STANDARDWOFFPACK_STUDENT but also the associated name "Office A1 for students".