Konverion

Microsoft 365Checker Manual

Version 7

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
Fidor Bank AG
IBAN: DE85 7002 2200 0020 3410 68
BIC: FDDODEMMXXX

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 use the Microsoft 365Checker sensibly, you need a user account in your Microsoft 365Tenant that has read access to the configuration of the services to be checked.

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 365Checker to read configurations in your Microsoft 365Tenant, it needs appropriate rights. The easiest way to do this is to use the “Global Reader” role predefined in Microsoft 365. This role may read all settings in Microsoft 365, with the exception of eDiscovery searches and "Data Subject Requests" in the GDPR Dashboard. To be able to read the Audit Logs, the account must be assigned the “Security Reader” role additionally.

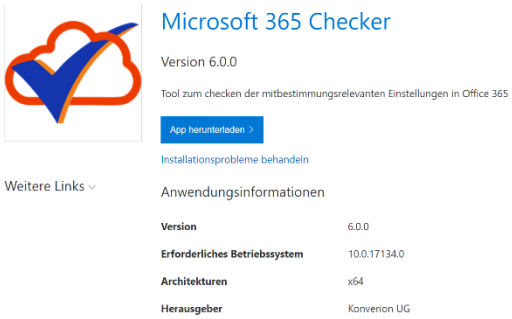
To use the Microsoft 365Checkers, it is useful to create a separate account in Microsoft 365and assign the required rights to it. In this way, the use of the Checker can also be traced in the Microsoft 365 Audit log.

For the purposes of this manual, the account "braudit@zusenberg.de" is used.

For the installation of the necessary Powershell modules you must also have administrator rights on the local PC. But this is only necessary for the installation of the Powershell modules. To run Microsoft 365 Checker, you do not need these administrative privileges.

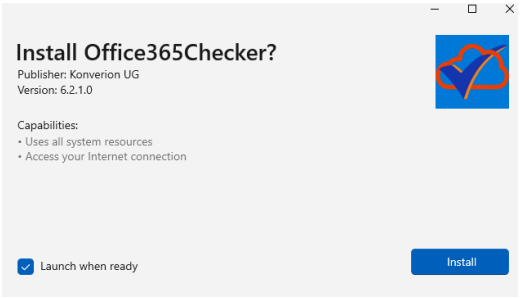
Installation

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.

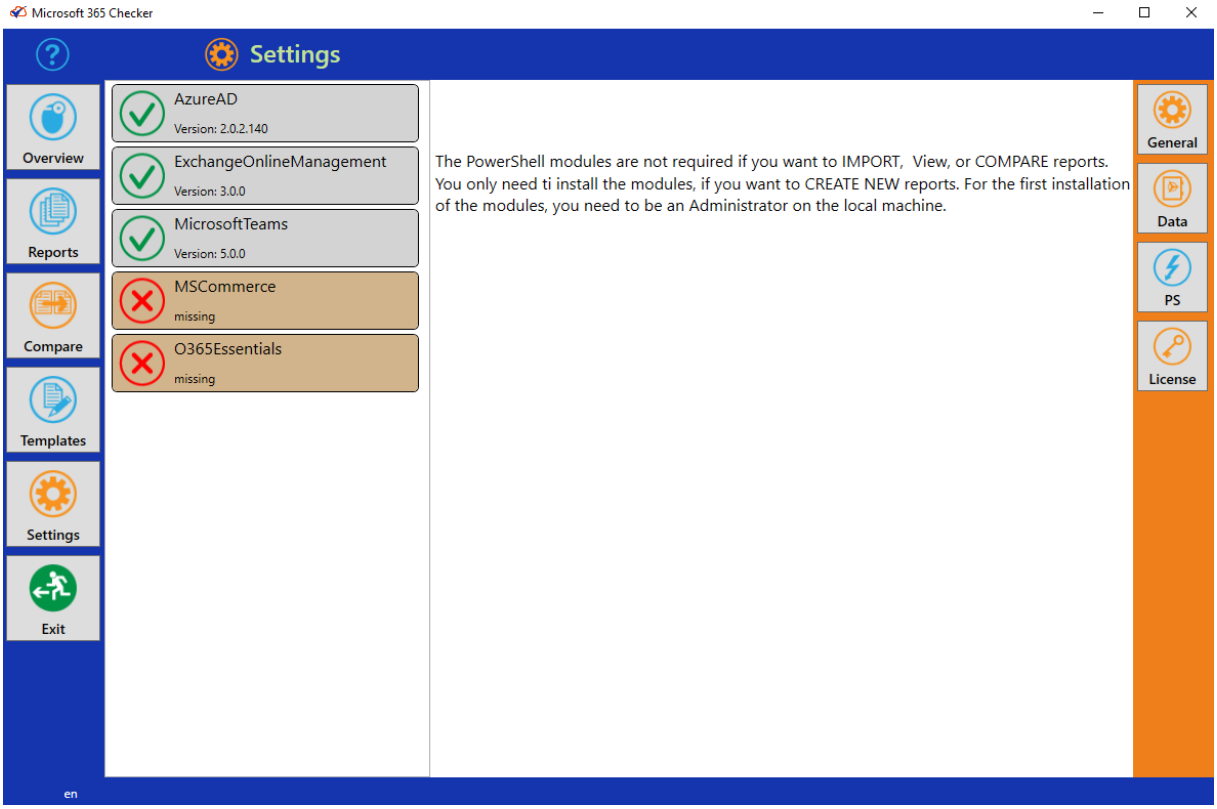
After download click on “Open file”.



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 - without IT involvement - can install certain products. For paid products, these can be paid for with a private credit card.

For which products self-service purchases are allowed, see 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 include the self-service purchases in a report, you will always be prompted for a login again when generating the report.

By requiring an interactive login, the "MSCommerce" module cannot be used in encapsulated mode.

Hopefully, in the future Microsoft will bring this module in line with the standards of the other PowerShell modules so that separate authentication is no longer necessary.

If you want to read the settings for self-service purchases, click the "MSCommerce" button. The module will then be installed and can also be found in the "c:\data\office365checker\PS" folder afterwards.

"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.

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".

Encapsulated Mode

As described in the section "Preparation", you need a user account that has read permission for as many settings in the Microsoft 365Tenant as possible to use the Microsoft 365Checker. The easiest way to do this is via the "Global Reader" role.

In larger companies in particular, however, there are often reservations about providing the works council with an account with such extensive read rights, since this would also allow to view the configuration (not the contents!) of manager accounts, for example.

In order to provide a solution that is viable for both sides, an "encapsulated mode" has been integrated into Microsoft 365Checker. In this mode, the user account with the "Global Reader" authorization can only be used in conjunction with Microsoft 365Checker. Direct access to the Microsoft 365Tenant via this account is therefore no longer possible.

In this way, the information requirements of the works council on the one hand, and the security requirements of IT on the other, can be satisfied.

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

Multi-factor authentication

As of version 5.4, support for accounts with multi-factor authentication (MFA) is possible for the use of Microsoft 365 Checker.

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

Therefore, since version 5.4 of the checker, it is also possible to use the filter options independently of the encapsulated mode.

Thus, with multi-factor authentication enabled, reports can be created and exported by IT to suit each works council committee. Since exported reports are encrypted and have a hashed checksum, it is not possible to tamper with exports.

To learn how to use encapsulated mode without sacrificing second-factor security, see the following section.

Conditional access Policies

Since encapsulated mode and multi-factor authentication are technically mutually exclusive, conditional access policies provide a solution.

This allows standard interactive MFA procedures to be replaced by a "static" second factor. Depending on the technology used, the second factor can be, for example, permitted IP addresses/ranges or devices registered in Azure AD.

So, to also be able to use encapsulated mode with a second authentication factor, disable multi-factor authentication for the account that is intended for works council controls.

Then, create a conditional access policy that allows logins from only defined IP addresses for that account.

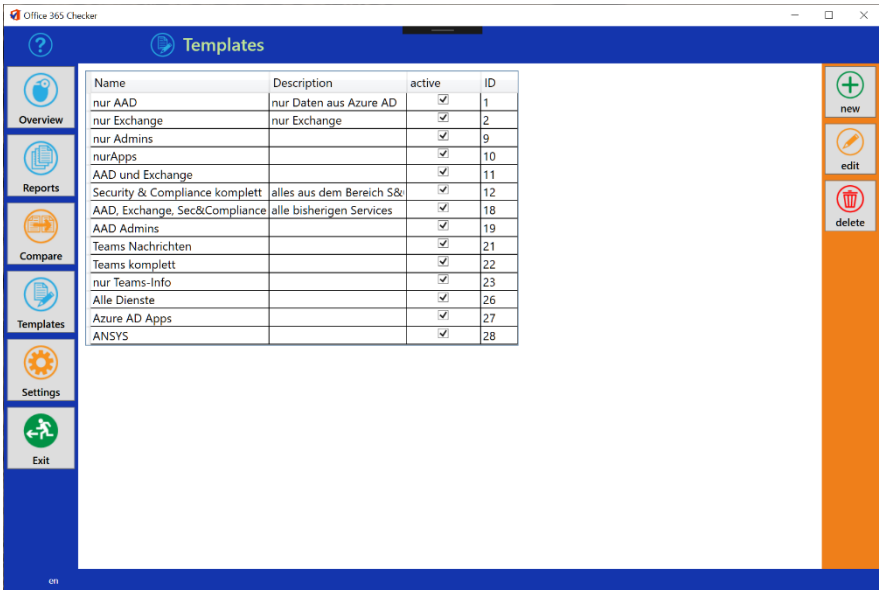
For more information on how to disable MFA for individual user accounts and create conditional access policies, see here : https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa

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 

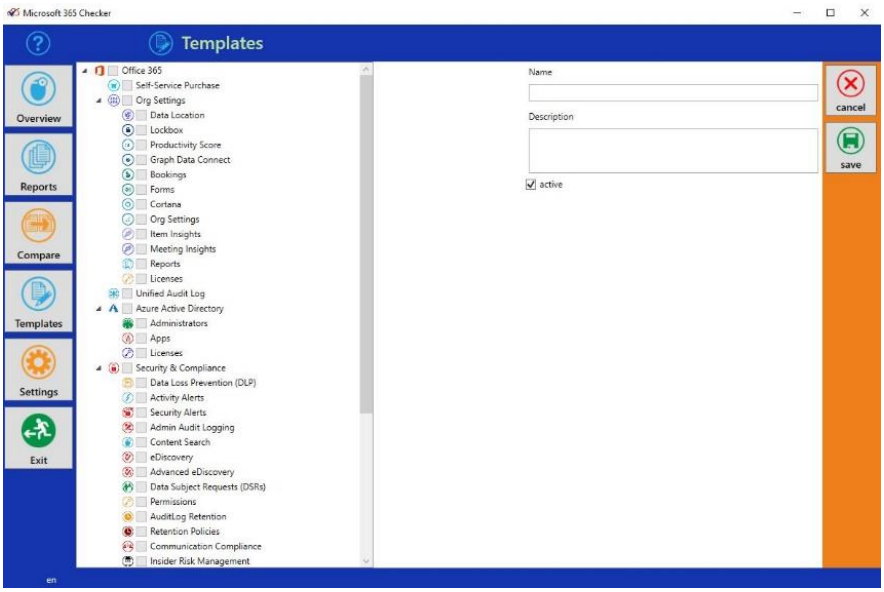


A view of the templates already defined is displayed:

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.

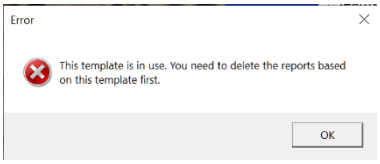
Edit templates

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.

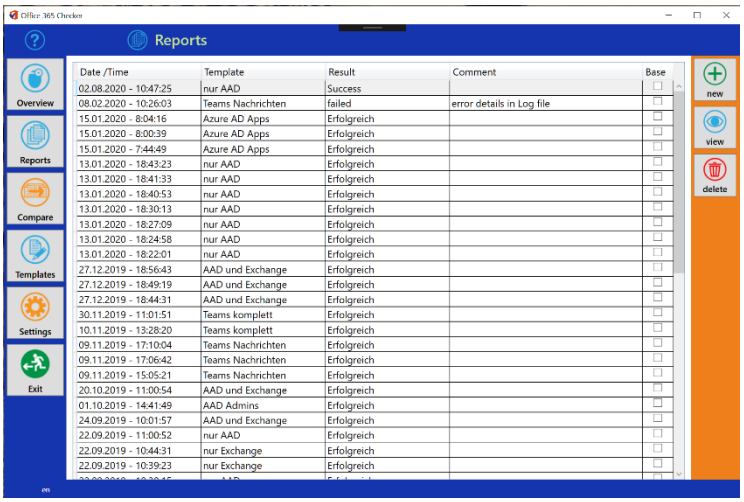


If reports have already been created with the selected template, the system displays a corresponding message:

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

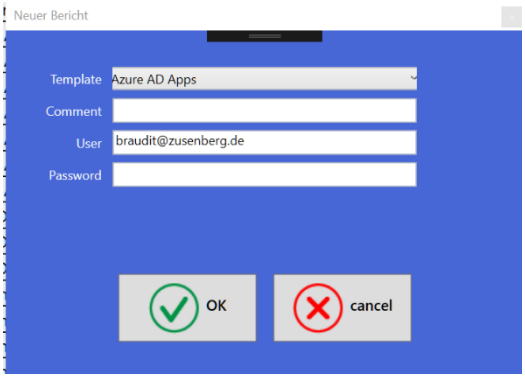
The configurations read from Microsoft 365are compiled in reports. To work with reports, click on the "Reports" section.



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

To create a new report, click on the "new" function button. A dialog box appears.



If you click on the "Template" selection field, a list of all defined templates with the status "active" is displayed. Select the desired template on the basis of which you want to create a report. You can 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 will need to enter a user account and password that will be used by Microsoft 365 Checker to log in to your Microsoft 365 Tenant.

To successfully create a report, the specified account must have read permissions for the services compiled in the selected template. It makes sense to use an account with the "Global Reader" permission in Office 365.

You can preset the user name in the Microsoft 365 Checkers settings. The password is never saved.

Click OK, and Microsoft 365 Checker begins generating the report.

The rotating Microsoft 365 Checker logo is briefly displayed and the message "Report being created" is displayed.

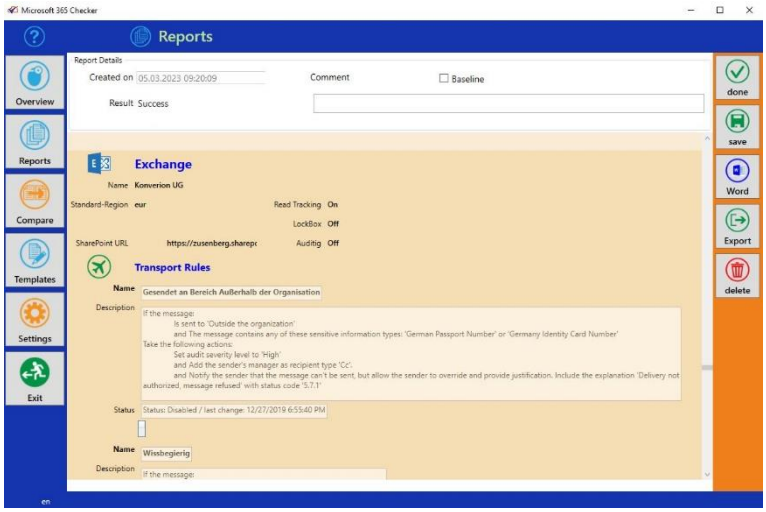
Depending on the number of configurations to be read, the creation of a report may take several minutes.

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

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 "Basisline" 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.

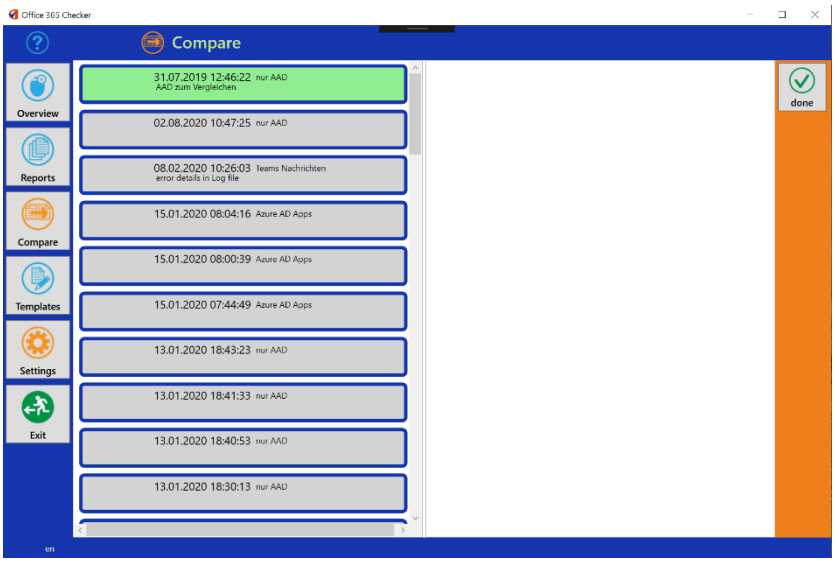
Tip:

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.

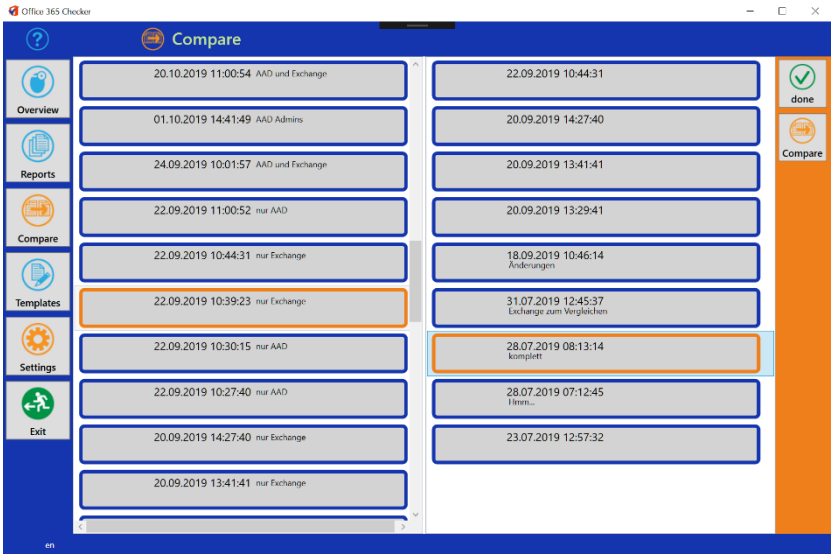


To compare reports with each other, select the "Compare" section.

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.



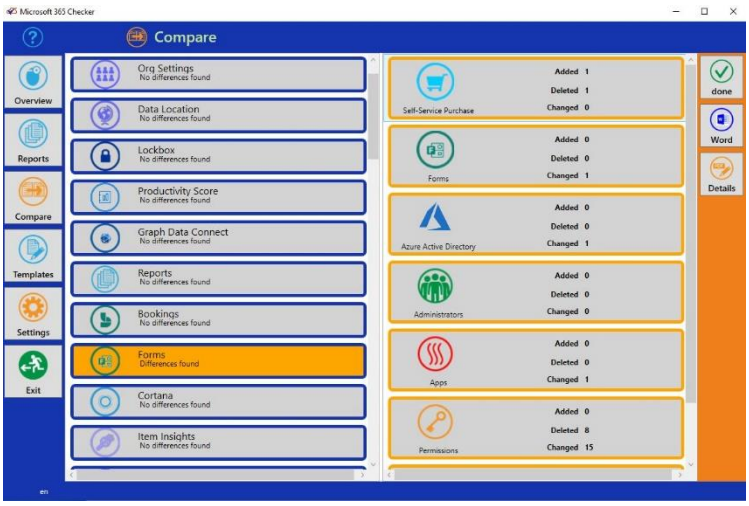
From the list on the right, select the report with which the orange marked report of the left list is to be compared.

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.

Use Encapsulated Mode (not in combination with MFA)

Encapsulated mode restricts the use of the user account that has the read permissions to configure the tenant to the Microsoft 365Checker.

Normally, the works council is given an account with the "Global Reader" permission to exercise its control rights (example: braudit@zusenberg.de).This account also allows logon to the various Microsoft 365Admin Centers, so that access to the configuration of the accounts of executives is also 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, and an encryption password that allows the Microsoft 365Checker to decrypt the file.

The file itself (Office365Checker.locked) contains the hash value of the user name and the corresponding password. Even if this file were to fall 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 to use the Microsoft 365Checkers

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

So there is no way to log on to Microsoft 365directly with this account.

To use this mode, follow these steps:

1. IT creates the user account
1. (in the example: braudit@zuenberg.de with password "!top9Secret")
2. the IT department uses the Microsoft 365Checker to create the file "Office365Checker.locked" with the encryption password "#IT.encrypted!
3. the works council receives:
    a. the user name "braudit@zusenberg.de"
    b. the Office365Checker.locked file
    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, Microsoft 365Checker recognizes the file and prompts for the user name and encryption password.
6. the encryption password is used to decrypt the file and read the user password "!top9Secret". The program also checks whether the user name entered corresponds to the user name stored as a hash value in the file.

The Microsoft 365Checker logs on to Microsoft 365with the account braudit@zuenberg.de and password "!top9Secret" and generates the desired reports.

Limiting the results in encapsulated mode

If you use the encapsulated mode, you can restrict the display of personal data (name, email address, ...) in the reports.

This is useful, for example, if you want to include only the data of German users in the reports in an international company, since only these users are represented by the works council. Even if several German companies are grouped together 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 fields "CompanyName", "Country or Region" or "UsageLocation".

Example:

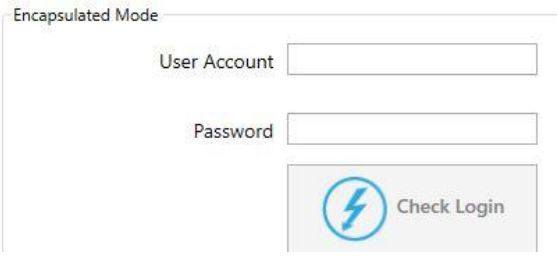
In the tenant of an international company, the country code is filled in for all users in the "Country or Region" attribute according to the employee's location. For all users residing in Germany, this is "DE".

If you now create an "Office365Checker.locked" file with the restriction "Country=DE", only user names of German employees will be displayed in the reports under the items "Journal" or "Litigation Hold". For all others, "Anonymous" appears.

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

Creating the Office365Checker.locked file

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



In the "Encapsulated Mode" area, enter the user name (in the example: braudit@zusenberg.de" and the corresponding password (in the example: "!top9Secret"). Click on the "Check login" button. The Microsoft 365 Checker will then test the logon to your Microsoft 365 Tenant with the information provided. If the login was successful, an input field for the encryption password appears and the button changes to "Create file".

If you select the "Restrict results" checkbox, you can then specify which field the restriction should be based on.

You can also specify that only the number of administrators in each role is displayed.

This information is also encrypted in the Office365Checker.locked file, and cannot be changed by the subsequent user.

Enter the encryption password (in the example: "#IT.encrypted!") and click "Create file".

Attention: the encryption password is shown in plain text until the file is saved.

A dialog box appears where you can select where the file should be saved.
Now you can make the saved file available to the works council. The works council places it in the folder "C:\data\Office365Checker" on the computer on which Microsoft 365Checker is to run.

Also tell the works council the user name and the encryption password.

Creating Reports in Encapsulated Mode

Click on the "Reports" area and then on the "+New" button.

If the file "Office365Checker" exists in the directory "C:\data\Office365Checker", a special dialog box for creating 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 is created.

Require a second Authentication factor for encapsulated mode

Since multi-factor authentication always requires an interactive login, user accounts for which MFA is enabled cannot be used for encapsulated mode.

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 allows you to require as a second factor, for example, a specific IP address)/range, or even a registered PC (requires the use of Microsoft Intune).

Proceed as follows (example for restriction to a specific IP address):

Create the desired user account (in the example "braudit-ip@zusenberg.de"), and assign it the roles "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 policy).

In Azure Active Directory, create a named location in the Conditional Access section. Here you can specify the IP address or IP range from which the account can log in. For example, you can ensure that logon is only possible from the corporate network.

Next, create a new conditional access policy.

As the user, enter the BR control account.

Under "Cloud apps and actions", select "All cloud apps".

For "Condition", under "Locations", enter "All Locations" for "Include", and for "Exclude", enter the location you just created.

Under "Grant", enter "Block access".

Switch "Enable Policy" to "On" (or "Report Only" if you want to test it first).

Click on "save".

If you want to test the policy, click the corresponding policy and select "WhatIf" from the top menu bar.

Here you can test when and how the policy takes effect by specifying different user names / IP addresses.

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

Settings

The category "Settings" is currently divided into four 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

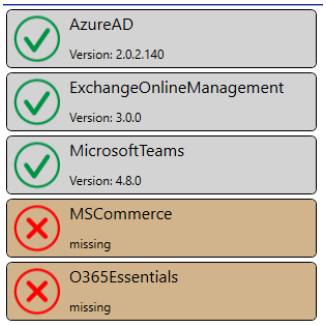
Here you can see the current path to the database (Office365Checker.sdf) If necessary, you can move the database to another hard disk or directory by clicking the "move" button. However, as long as there are no weighty reasons, you should leave the database where it is.

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.

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.

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 for the following categories are read from the Unified Audit Log:

eDiscovery
Advanced eDiscovery
Settings for anonymization of Usage-reports
Add member to administrative role
Remove member from administrative role
WorkplaceAnalytics

To keep the reports clear, the actions performed are summarized and the total number of actions is recorded.

The meaning of „Operations“ is explained here: https://docs.microsoft.com/de-de/microsoft-365/compliance/search-for-ediscovery-activities-in-the-audit-log?view=o365-worldwide

For anonymization od Usage-reports and adding or removing users to an administrative role, the records are shown in detail.

Anonymization of 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 anonymization of Usage reports was turned off by user „joergsc@zusenberg.de“, on the same day at 22:44 it was turned on again.

Add administrative roles:

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 the user braudittest@zusenberg.de was added to the role „User Account Administrator“ from joergsc@zusenberg.de.

Removing administrative roles:

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 11:14 the user braudittest@zusenberg.de was removed from the role „Global Reader“ by user joergsc@zusenberg.de.

Azure Active Directory

Info

Tenant Name
Address (street, postcode, city)
Country
Phone
Privacy ContactURL
Number of User

AAD roles

All roles with:
Name
Description
Role owners
with name, first name and email address

AAD apps

All registered apps with:
Name
Description
Owner
Permissions
Note: Permissions to the Microsoft Graph API are highlighted

AAD Administrative Units

All administrative units with Membership Rule, Count of assigned Users, Groups and Devices, as well as Administrators. For Count of Users, Groups and devices and listing of Administrators. The “AzureADPreview” PowerShell Modul is required.

Privileged Identity Management

If E5 licenses are available in the tenant, "Privileged Identity Management (PIM)" can be used for a large number of roles. This can be used to ensure that administrators do not have standing authorizations, but are only granted authorizations when they are specifically required. Administrators are therefore no longer assigned directly to an AzureAD role, but managed via PIM. There are two options for assignments to a role: "active" or "eligible".

If an assignment is "active", it does not need to be requested separately. So it is more or less the same as a direct assignment to a role. However, the start and end date of the assignment can be defined via PIM, so that the authorizations are only available for a certain period of time.

If an assignment is "eligible", the administrator must request the authorization via a web page. Approval can be automatic or granted by specified individuals.

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

All available roles are listed with assignments (if there are any).

Microsoft 365Security & Compliance

Data Loss Prevention DLP

All DLP rules with:
Name
Description
Status
Mode
Areas affected (Exchange, SharePoint, OneDrive for Business, Teams)

Activity notifications

All activity notifications with:
Name
Description
Operation
Message to

Security alerts

All security notifications with:
Name
Description
Operation
Message to

Content search

All content searches with:
Name
Description
Search for
Created by
Last changed
Included and excluded areas

eDiscovery

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

Name
Description
Status
Last changed by
Case Admin

Advanced eDiscovery

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

Name
Description
Status
Last changed by
Case Admin

Data Subject Requests

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

Name
Description
Status
Created on
Last modification by
Editor

Information-Barriers

All Information Barrier Segments and Policies

Rolls

All Microsoft 365roles with:
Name
Description
Members
(display name, surname, first name, email address)

Exchange

Info

Name of the organization
Standard region
SharePoint URL
Read Tracking
LockBox
Auditing

Transport rules

All transport rules with:
Name
Description
Status
Last change

Data Loss Prevention

All DLP rules with:
Name
Description
Status
Mode

Journal

All journal rules with:
Name
Monitored mailbox / distribution list
Journal Recipient

Scope
Mode
Last changed

eDiscovery

All Exchange eDiscoveries with:
Name
Description
Source
Last run by
Last run

Teams

Message Policies

All message policies with:
Name
Description
Owner can delete messages
User can delete messages
User can modify messages
Translation
URL Preview

Meeting Policies

All meeting policies with:

Name
Description
All settings

Live Event Policies

All live event policies with:
Name
Description
All settings

App Permissions

All app permission policies with:
Name
Description
Standard App Catalog
Global App Catalog
Private App Catalog
Catalog Types

Compliance Recording Policies

All compliance recording Policies with:
Name
Description

Status
Registered application

Self-Service Purchase

The list of all products available for Self-service purchase:

Produkt	Setting	ProductID
Power Apps per user	Enabled	CFQ7TTC0LH2H
Power Automate per user	Enabled	CFQ7TTC0KP0N
Power Automate RPA	Enabled	CFQ7TTC0KXG6
Power BI Premium (standalone)	Enabled	CFQ7TTC0KXG7
Power BI Pro	Enabled	CFQ7TTC0L3PB
Project Plan 1	Enabled	CFQ7TTC0HDB1
Project Plan 3	Enabled	CFQ7TTC0HDB0
Visio Plan 1	Enabled	CFQ7TTC0HD33
Visio Plan 2	Enabled	CFQ7TTC0HD32
Viva Goals	Enabled	CFQ7TTC0PW0V
Windows 365 Enterprise	Enabled	CFQ7TTC0HHS9
Windows 365 Business	Enabled	CFQ7TTC0J203
Windows 365 Business with Windows Hybrid Benefit	Enabled	CFQ7TTC0HX99
Microsoft 365 F3	Enabled	CFQ7TTC0LH05
Dynamics 365 Marketing	Enabled	CFQ7TTC0LH3N
Dynamics 365 Marketing Attach	Enabled	CFQ7TTC0LHWP
Dynamics 365 Marketing Additional Application	Enabled	CFQ7TTC0LHVK
Dynamics 365 Marketing Additional Non-Prod Application	Enabled	CFQ7TTC0LHWM

Setting	**Auswirkung**
Enabled	Users can perform self-service purchases and can register for trial versions
OnlyTrialsWithoutPaymentMethod	Users cannot perform self-service purchases, but can register for trial versions, that do not require a payment method.
Disabled	Users cannot perform self-service purchases and cannot register for trial versions.

Org Settings

General Settings

Primary Tenant Name
Notification Language
Technical contact
Privacy contact
Privacy-URL

Data Location

Data Location (data-at-rest location) for
Exchange
SharePoint
Teams

Multi-Geo in use (true/false)

Lockbox

Customer-Lockbox activated (true / false)

Productivity Score

Parameter	
ProductivityScoreOptedIn	
OperationUserPuid	
OperationTime	

Graph Data Connect

Parameter	
ServiceEnabled	
TenantLockBoxApproverGroup	
TenantLockBoxDataAccessPolicyType	
IsOdspEnabled	
IsCrossTenantDataMovementEnabled	
IsVivaInsightsEnabled	

Usage Reports

Parameter	
GraphApiEnabled	
PowerBiEnabled	
PrivacyEnabled	
Region	
TenantId	
PBIStatusUpdateDate	
PBIStatus	

Bookings

Parameter	
Enabled	
SocialSharingRestricted	
BookingsExposureOfStaffDetailsRestricted	
StaffMembershipApprovalRequired	
BookingsSmsMicrosoftEnabled	
BookingsSearchEngineIndexEnabled	
BookingsNamingPolicyEnabled	
Weitere Parameter	

Forms

Parameter	
ExternalCollaborationEnabled	
ExternalSendFormEnabled	
ExternalShareCollaborationEnabled	
ExternalShareTemplateEnabled	
ExternalShareResultEnabled	
RecordIdentityByDefaultEnabled	
BingImageSearchEnabled	
InOrgFormsPhishingScanEnabled	
InOrgSurveyIncentiveEnabled	

Cortana

Parameter	
Enabled	

MyAnalytics

Diese Einstellungen gelten für alle Benutzer.

Parameter	
EnableInsightsDashboard	
EnableWeeklyDigest	
EnableInsightsOutlookAddIn	

Elementeinblicke

Parameter	
AllowItemInsights	
DisabledForGroup	
DisabledForGroupID	

Besprechungseinblicke

Parameter	
AllowMeetingInsights	

Licenses

Same information as „Licenses“ in the AzureAD section, but including the product name (not SKU only)

For example not only STANDARDWOFFPACK_STUDENT but the name „Office A1 for students“.