Konverion

# Microsoft 365 Checker

# Handbuch

## Version 8.0

Konverion UG (haftungsbeschränkt)
Markelstrasse 48
12163 Berlin
Geschäftsführer: Jörg Schanko

Amtsgericht Berlin-Charlottenburg
HRB: 195062 B
St-Nr: 29/392/30664
USt-ID: DE317517149

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

# Inhalt

Vorwort ..... 6
Hinweis zu älteren Versionen des Checkers (7.x) ..... 6
Telemetrie ..... 6
Lizensierung ..... 7
Vorbereitung ..... 8
Installation ..... 9
„MSCommerce“ PowerShell Modul ..... 11
„O365Essentials“ PowerShell Modul ..... 11
„AzureADPreview“ PowerShell Modul ..... 12
Generelle Vorgehensweise ..... 13
Vorlagen erstellen ..... 14
Eine neue Vorlage erstellen ..... 14
Vorlagen bearbeiten ..... 15
Vorlagen löschen ..... 15
Berichte erstellen ..... 16
Neue Berichte erstellen ..... 16
Berichte ansehen ..... 17
Gefilterte Berichte ansehen ..... 18
Vergleichsgrundlage festlegen ..... 18
Bericht als Word Dokument speichern ..... 19
Bericht löschen ..... 19
Bericht exportieren ..... 19
Bericht importieren ..... 20
Berichte vergleichen ..... 21
Detailvergleich ..... 22
Übersicht des Vergleichs in Word exportieren ..... 23
Einstellungen ..... 24
Allgemein ..... 24
Daten ..... 24
PS (PowerShell) ..... 25
Microsoft Graph ..... 25
Anwendung in Entra ID registrieren ..... 25
Berechtigungstypen ..... 28
Microsoft 365 Checker für Graph konfigurieren ..... 29
Zertifikat-basierte Anmeldung einrichten ..... 29

Lizenz ..... 33
Übersicht ..... 33
Veraltete Funktionen nutzen (Checker Version 7.x) ..... 34
Gekapselter Modus ..... 34
Multi-Faktor-Authentifizierung ..... 34
Richtlinien für bedingten Zugriff ..... 34
Einen neuen Bericht erstellen ..... 35
Gekapselten Modus verwenden ..... 37
Einschränken der Ergebnisse ..... 39
Erstellen der „Office365Checker.o3c“ Datei ..... 40
Berichte im gekapselten Modus erstellen ..... 41
Den gekapselten Modus mit einem zweiten Authentifizierungs-Faktor absichern ..... 41
Problembehandlung ..... 43
Der Microsoft 365 Checker lässt sich nicht installieren ..... 43
Installation der PowerShell Module ..... 43
Security & Compliance Einstellungen werden nicht gelesen ..... 44
Anhang: Auslesbare Einstellungen ..... 45
Unified Audit Log ..... 45
Azure Active Directory ..... 46
Info ..... 46
AAD Rollen ..... 46
AAD Apps ..... 46
AAD Verwaltungseinheiten ..... 46
Privileged Identity Management ..... 47
Lizenzen ..... 48
Microsoft 365 Security & Compliance ..... 48
Data Loss Prevention DLP (Verhindern von Datenverlust) ..... 48
Aktivitätsbenachrichtigungen ..... 48
Sicherheitsbenachrichtigungen ..... 48
AuditLog Aufbewahrungsrichtlinien ..... 48
Aufbewahrungsrichtlinien ..... 49
Kommunikations-Konformität ..... 49
Insider Risiko Management ..... 49
Inhaltssuche ..... 49
eDiscovery ..... 49
Advanced eDiscovery ..... 50

Data Subject Requests ..... 50
Compliance Grenzen ..... 50
Informations-Barrieren ..... 50
Rollen ..... 51
Exchange ..... 51
Info ..... 51
Transportregeln ..... 51
Data Loss Prevention ..... 51
Journal ..... 51
eDiscovery ..... 51
Aufbewahrungsrichtlinien ..... 52
Teams ..... 53
Nachrichtenrichtlinien ..... 53
Besprechungsrichtlinien ..... 55
Webinar Richtlinien ..... 59
Liveereignis-Richtlinien ..... 59
KI-Richtlinien ..... 59
App Berechtigungen ..... 60
Richtlinien zur Compliance Aufzeichnungen ..... 60
Microsoft Viva ..... 60
Viva Insights ..... 60
Selbstbedienungseinkäufe ..... 61
Einstellungen der Organisation ..... 62
Generelle Einstellungen ..... 62
Datenspeicherort ..... 62
Lockbox ..... 62
Einführungsbewertung ..... 62
Graph Data Connect ..... 62
Berichte ..... 62
Bookings ..... 63
Forms ..... 63
Cortana ..... 64
MyAnalytics ..... 64
Elementeinblicke ..... 64
Besprechungseinblicke ..... 65
Lizenzen ..... 65

## Vorwort

Der Microsoft 365 Checker ist ein Hilfsprogramm, das in erster Linie Betriebsräte aber auch Compliance- und Datenschutzbeauftragte dabei unterstützen soll, die in den zahlreichen Komponenten von Microsoft 365 vorgenommenen Konfigurationen zu überwachen.

So kann zum Beispiel auf einfache Art und Weise festgestellt werden, ob die in einer Betriebsvereinbarung niedergelegten Regelungen auch konsistent umgesetzt werden. Der Microsoft 365 Checker greift dabei ausschließlich lesend auf den jeweiligen Microsoft 365 Tenant zu. Die gelesenen Konfigurationen werden auf dem lokalen PC in einer verschlüsselten Datenbank gespeichert. So können die Konfigurationsstände zu verschiedenen Zeiten miteinander verglichen und Unterschiede sichtbar gemacht werden.

Um den Microsoft 365 Checker sinnvoll nutzen zu können, benötigt man in seinem Microsoft 365 Tenant entweder ein Benutzerkonto mit ausreichenden administrativen Berechtigungen, oder eine Registrierte Anwendung in Entra ID.
Beide Vorgehensweisen und die dafür benötigten Konfigurationen werden im Abschnitt „Vorbereitung“ beschrieben.

## Hinweis zu älteren Versionen des Checkers (7.x)

Microsoft hat zwei wesentliche Änderungen angekündigt, die Einfluss auf die Funktion des Checkers haben.

1. Die AzureAD und AzureAD Preview PowerShell Module werden zum März 2025 eingestellt. Als Ersatz dienen die „Microsoft Graph PowerShell“ Module. Diese erfordern das Registrieren einer Anwendung in Entra ID.
   Für den Checker haben wir auf die Nutzung der Microsoft Graph PowerShell Module verzichtet, und greifen direkt über den Microsoft Graph zu. Das erhöht die Geschwindigkeit und reduziert Komplexität.
   Mit der Version 8 des Checkers kann also bereits auf die AzureAD bzw. AzureAD Preview PowerShell Module verzichtet werden.
2. Alle Benutzerkonten mit administrativen Berechtigungen erfordern ab Anfang 2025 Multi-Faktor-Authentifizierung MFA (bereits jetzt umgesetzt für den Zugriff auf jegliche administrativen Webseiten).
   Damit kann der „gekapselte Modus“ der älteren Checker Versionen nicht mehr funktionieren, da MFA immer eine interaktive Anmeldung erfordert.
   Um eine mit dem gekapselten Modus vergleichbare Funktionalität anzubieten, kann man ab der Version 8 auf eine Zertifikat-basierte Anmeldung wechseln.

Die Version 8 des Checkers unterstützt auch noch alle Möglichkeiten der älteren Versionen, solange dies technisch möglich ist. Es ist aber allein aus Geschwindigkeitsgründen sinnvoll, bereits jetzt auf die Graph-gestützten Funktionen zu wechseln.

## Telemetrie

Telemetrie ist eine hervorragende Methode, die notwendigen Daten zu sammeln, aufgrund derer man ein Fehler in einem Programm beheben und Funktionen verbessern kann.

Da der Microsoft 365 Checker jedoch sensible Informationen über die Konfiguration eines Microsoft 365 Tenant ausliest, haben wir vollständig auf Telemetrie verzichtet. Mit anderen Worten: der Microsoft 365 Checker „telefoniert nicht nach Hause“. Weder zur Produktverbesserung, noch zur

Lizenzkontrolle, noch sonst wie. Den einzigen Kontakt zu unserem Server nimmt der Checker beim Start auf um zu sehen, ob eine neue Version verfügbar ist.

Der Verzicht auf jegliche Art Telemetrie bedeutet aber auch, dass wir zur Verbesserung des Microsoft 365 Checkers auf das Feedback der Benutzer angewiesen sind.
Wenn Sie also Fehler finden, eine Funktion nicht so ist, wie Sie sie gerne hätten, oder nicht vorhanden ist – schicken Sie eine E-Mail an support@konverion.de. DANKE!

## Lizensierung

Um festzustellen, ob der Microsoft 365 Checker Ihren Erwartungen entspricht und die Funktionen bietet, die Sie benötigen, können Sie ihn 30 Tage lang testen. Dazu ist keinerlei Registrierung oder ähnliches notwendig. Während des Testzeitraumes stehen Ihnen alle Funktionen uneingeschränkt zur Verfügung.

Nach Ablauf der 30 Tage können Sie keine neuen Berichte mehr erstellen. Auf bereits erstellte Berichte können Sie jedoch nach wie vor Zugreifen.

Um nach Ablauf des Testzeitraumes weiterhin neue Berichte erstellen zu können, müssen Sie eine Lizenz des Microsoft 365 Checkers erwerben. Dazu können Sie das auf unserer Webseite hinterlegte Bestellformular verwenden (https://konverion.de/images/Bestellung_Office_365_Checker.docx) .

Mit dem Erwerb eine Lizenz erhalten Sie das Recht, den Microsoft 365 Checker auf beliebig vielen PCs einzusetzen. Die Lizenz ist auch nicht auf eine bestimmte Anzahl Benutzer beschränkt.

Nach Eingang der Bestellung senden wir Ihnen eine Lizenzdatei zu. Diese Lizenzdatei legen Sie auf jedem PC, auf dem mit dem Microsoft 365 Checker Berichte erstellt werden sollen, nach der Installation des Programmes im Datenverzeichnis („c:\data\Office365Checker“) ab. Auf PCs, die lediglich Berichte anzeigen und vergleichen sollen, benötigen Sie keine Lizenzdatei.

Weitere Informationen zum Thema Lizensierung finden sie auf unserer Webseite.

## Vorbereitung

Damit der Microsoft 365 Checker in Ihrem Microsoft 365 Tenant Konfigurationen auslesen kann, benötigt er entsprechende Berechtigungen und (derzeit noch) einige PowerShell Module.

Dies lässt sich am einfachsten über die in Microsoft 365 vordefinierte Rolle „Globaler Leser“ (englisch: „Global Reader“) erreichen. Diese Rolle darf sämtliche Einstellung in Microsoft 365 lesen, mit Ausnahme der eDiscovery Suchen und den „Anträgen betroffener Personen“ im DSGVO Dashboard. Um die Audit-Logs auswerten zu können, weisen Sie dem Benutzerkonto in Microsoft Purview die Rollen „Audit Manager“ zu.
Über die Einträge im Audit-Log kann dann auch festgestellt werden, ob eDiscovery Suchen o.ä. durchgeführt wurden.

Für die Nutzung des Microsoft 365 Checkers ist es sinnvoll, ein separates Konto in Microsoft 365 anzulegen, und diesem die benötigten Rechte zuzuweisen. So kann auch die Verwendung des Checker im Microsoft 365 Ereignisprotokoll nachvollzogen werden.

Im Rahmen dieses Handbuches wird die Konten „braudit@zusenberg.de“, bzw brauditMFA@zusenberg.de genutzt.

Wie Sie den Checker für die Nutzung der Microsoft Graph Programmierschnittstelle, oder die Zertifikat-basierte Anmeldung konfigurieren, lesen Sie im Abschnitt „Einstellungen – Graph“ bzw. „Einstellungen – Zertifikat“.

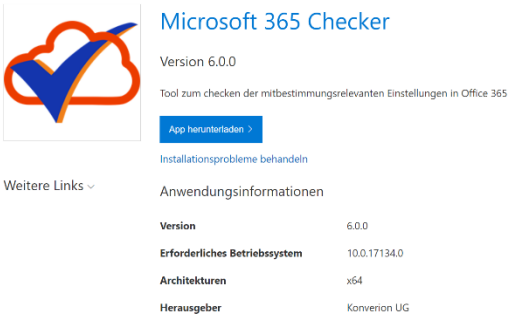
Für die initiale Installation der notwendigen PowerShell Module müssen Sie außerdem Administratorrechte auf dem lokalen PC haben. Dies ist aber nur für die Installation der „NuGet“ PowerShell Module notwendig. Diese werden benötigt, um Module in der Microsoft PowerShell Galerie (https://www.powershellgallery.com/) finden und herunterladen zu können. Um den Microsoft 365 Checker auszuführen, benötigen Sie diese Administratorrechte nicht.

Wenn Sie Berichte nur importieren, ansehen und vergleichen wollen, brauchen die PowerShell Module nicht installiert zu werden.

# Installation

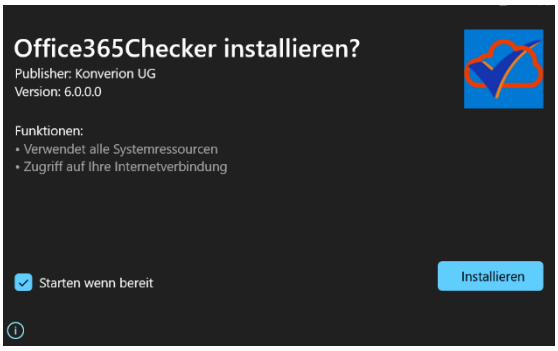
Der Microsoft 365 Checker wird durch sogenanntes „querladen“ installiert. Dieses muss auf Ihrem PC erlaubt sein. Stellen Sie unter „Einstellungen“ – „Update und Sicherheit“ – „Für Entwickler“ sicher, dass entweder „Apps querladen“, oder „Entwicklermodus“ aktiviert sind.

Starten Sie dann die Installation des Microsoft 365 Checkers durch Aufrufen der URL
https://www.konverion.de/Microsoft365Checker/index.html




Klicken Sie auf „App herunterladen“.

Das „Deployment“-Paket wird damit auf Ihren PC heruntergeladen. Klicken Sie anschließend auf „Datei öffnen“.

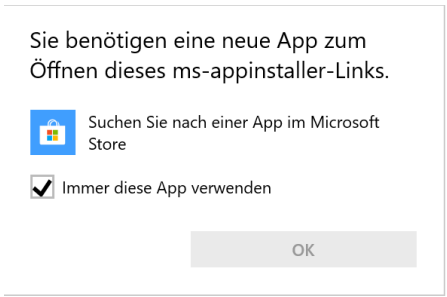



Es erscheint ein Dialogfenster, in dem Sie auf „Installieren“ klicken.

Der Microsoft 365 Checker wird nun installiert.

Bei der Installation legt der Microsoft 365 Checker ein Verzeichnis „c:\Data\Office365Checker“ an. In diesem Verzeichnis wird die verschlüsselte Datenbank (Office365Checker.db3) sowie die Log-Datei (Log.txt) erstellt. Außerdem wird ein Unterverzeichnis „Berichte“ erstellt, in das alle exportierten Berichte gespeichert werden.

Hinweis:
Sollten Sie diese Meldung erhalten




dann müssen Sie aus dem Microsoft Store zuerst den App-Installer herunterladen.

Der Link hierzu:
https://www.microsoft.com/store/productId/9NBLGGH4NNS1

Ist der Microsoft Store auf Ihrem PC nicht verfügbar, setzen Sie in der Registry den Eintrag HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStoreRequirePrivateStoreOnly auf 0

Nach dem ersten Start werden Sie auf die Einstellungsseite für die PowerShell Module geleitet.

Hier wird als erstes geprüft, ob der sogenannten „NuGet Provider“ installiert ist. Dieses Modul ist erforderlich, um PowerShell Module in der Microsoft Modul-Galerie finden und von dort installieren zu können. Zur Installation des NuGet Providers müssen Sie Administrator auf der lokalen Maschine sein. Waren Sie bei der Installation kein Administrator, so konnte der NuGet Provider nicht installiert werden.
Sie erhalten dann die Meldung:


Starten Sie in diesem Fall die Windows PowerShell ISE als Administrator, laden Sie das Script c:\data\office365checker\installNuGet.ps1 ünd führen es aus.

Wenn der NuGet Provider installiert ist, können Sie – bei Bedarf – die PowerShell Module installieren.

Klicken Sie dazu auf auf den Schalter „installieren“.
Die benötigten PowerShell Module werden im Ordner „C:\data\Office365Checker\PS“ abgelegt.
Nach erfolgreicher Installation sollte dieses Verzeichnis 3 Unterordner enthalten:

- AzureAD
- ExchangeOnlineManagement
- MicrosoftTeams

Sie sollten nun dieses Ergebnis sehen:

Zusätzlich zu den drei erforderlichen Modulen werden noch die optionalen Module „AzureADPreview“, „MSCommerce“ und „O365Essentials“ angezeigt, die nicht automatisch installiert werden.

## „MSCommerce“ PowerShell Modul

Das „MSCommerce“ PowerShell Modul kann Ihnen die Einstellungen für die sogenannten „Selbstbedienungs-Einkäufe“ anzeigen.

Wenn Selbstbedienungs-Einkäufe erlaubt sind, können Benutzer – ohne Beteiligung der IT-Abteilung – bestimmte Produkte installieren. Bei kostenpflichtigen Produkten können diese mit einer privaten Kreditkarte bezahlt werden.

Für welche Produkte Selbstbedienungs-Einkäufe möglich sind, können Sie der Tabelle „MSCommerce“ im Anhang „Auslesbare Einstellungen“ entnehmen.

Bei Verwendung des „MSCommerce“ PowerShell Moduls ist zu beachten, dass dieses immer eine eigene Anmeldung erfordert. Wenn Sie also das Modul installieren und die Selbstbedienungs-Einkäufe in einen Bericht integrieren, werden Sie bei der Erstellung des Berichtes immer erneut nach einer Anmeldung gefragt.

Durch die Erfordernis einer interaktiven Anmeldung kann das „MSCommerce“ Modul nicht mit der Zertifikat-basierten Anmeldung und nicht im gekapselten Modus genutzt werden.

Es bleibt zu hoffen, dass Microsoft dieses Modul in der Zukunft an die Standards der anderen PowerShell Module anpasst, sodass eine separate Authentifizierung nicht mehr notwendig ist.

Wenn Sie die Einstellungen zu den Selbstbedienungs-Einkäufen auslesen möchten, klicken Sie auf den Schalter „MSCommerce“. Das Modul wird dann installiert und findet sich anschließend ebenfalls im Ordner „c:\data\office365checker\PS“.
Wenn Sie den Checker für die Nutzung der Microsoft Graph Programmierschnittstelle eingerichtet haben, brauchen Sie das MSCommerce PowerShell Modul nicht zu installieren, da die Einstellungen über die Graph-API ausgelesen werden können.

## „O365Essentials“ PowerShell Modul

Dieses Modul gehört zu den optionalen PowerShell Modulen, weil es undokumentierte Funktionen der Microsoft Programmierschnittstellen (API) benutzt und nicht von Microsoft selbst stammt. Derzeit stellt dies den einzigen Weg dar, die Organisationseinstellungen automatisiert auszulesen.

O365Essentials“ ist ein OpenSource Projekt der Firma „EvotecIT“. Der Quellcode findet sich auf GitHub https://github.com/EvotecIT/O365Essentials.

Die dauerhafte Funktion dieses Moduls kann aufgrund der genutzten undokumentierten Funktionen nicht gewährleistet werden.

Zu den Organisationseinstellungen gehören unter anderem der Datenspeicherort, die Einstellungen zu Forms, Bookings, MyAnalytics., etc. Die vollständige Liste der auslesbaren Organisationseinstellungen finden Sie im Anhang „Auslesbare Einstellungen“ unter „Einstellungen der Organisation“.

Wenn Sie die Einstellungen der Organisation auslesen möchten, klicken Sie auf den Schalter „O365Essentials“. Das Modul wird dann installiert und findet sich anschließend ebenfalls im Ordner „c:\data\office365checker\PS“. Für das Auslesen der Organisationseinstellungen sollte immer eine

separate Vorlage erstellt werden, die keine weiteren Dienste ausliest. Werden die Organisationseinstellungen mit anderen Diensten in einer Vorlage zusammengefasst, kommt es beim Erstellen eines Berichts gelegentlich zu Anmeldeproblemen. Die Organisationseinstellungen können dann nicht ausgelesen werden. Das Fehlerprotokoll (log.txt) enthält dann einen entsprechenden Hinweis.

## „AzureADPreview“ PowerShell Modul

Hinweis:
Das „AzureADPreview“ PowerShell Modul wird zum 30.März 2025 eingestellt. Wenn Sie die Microsoft Graph Programmierschnittstelle für den Checker benutzen, ist eine Installation des Moduls nicht erforderlich.

Das AzureADPreview PowerShell Modul ist nur notwendig, um die erweiterten Eigenschaften von Azure AD Verwaltungseinheiten und die Einstellungen zum „Privileged Identity Management (PIM)“ auszulesen. OB Verwaltungseinheiten eingerichtet sind, kann auch das AzureAD Modul erkennen. Die zugeordneten Mitglieder und Administratoren, sowie die Anzahl der in der Verwaltungseinheit enthaltenen Benutzer, Gruppen und Geräte sowie ggf. die dynamische Erstellungsregel können nur über das Preview Modul gelesen werden.
Wenn Sie Verwaltungseinheiten und PIM nicht benutzen gibt es keinen Grund, das AzureADPreview Modul zu installieren.

Wenn Sie auf die Schaltfläche für das AzureADPreview Modul klicken, wird dieses nach einer Sicherheitsabfrage installiert, und das AzureAD Modul wird deinstalliert. Falls Sie zuvor schon einen Bericht erstellt haben, der das Azure AD umfasst kann es vorkommen, dass das AzureAD Modul nicht gelöscht werden kann, da noch Dateien in Benutzung sind. Beenden Sie in diesem Fall den Checker und löschen Sie das Verzeichnis „c:\data\office365checker\PS\AzureAD“ von Hand.

Sie können jederzeit wieder das AzureAD Modul installieren, indem Sie auf die entsprechende Schaltfläche klicken. Das AzureADPreview Modul wird dann wieder deinstalliert. Die beiden Module schließen sich gegenseitig aus. Es kann also immer nur eins von beiden installiert sein.

Wenn alle notwendigen Powershell Module installiert sind können Sie mit der Arbeit mit dem Microsoft 365 Checker beginnen.

## Generelle Vorgehensweise

Um die Arbeit mit dem Microsoft 365 Checker so einfach wie möglich zu gestalten, gehen Sie wie folgt vor:

Über „Vorlagen“ legen Sie fest, welche Dienstkonfigurationen von Microsoft 365 Sie kontrolieren möchten. Sie können beliebig viele Vorlagen für unterschiedliche Anforderungen erstellen.
Die Erstellung von Vorlagen ist in „Vorlagen erstellen“ beschrieben.

1) Wenn Sie Ihre Vorlagen definiert haben, können Sie im Bereich „Berichte“ einen neuen, auf einer Ihrer Vorlagen basierenden Bericht erstellen.
   Die Erstellung von Berichten ist in „Berichte erstellen“ beschrieben.
2) Nachdem ein Bericht erstellt ist, können sie ihn als Word-Datei speichern oder drucken, um ihn beispielsweise mit der per Betriebsvereinbarung festgelegten Konfiguration zu vergleichen.
3) Um Veränderungen im Laufe der Zeit festzustellen, können Sie im Bereich „Vergleichen“ Berichte, die zu unterschiedlichen Zeiten erstellt wurden, miteinander vergleichen. Der Microsoft 365 Checker zeigt dann die festgestellten Veränderungen an.
   Die Vorgehensweise ist in „Berichte vergleichen“ beschrieben.

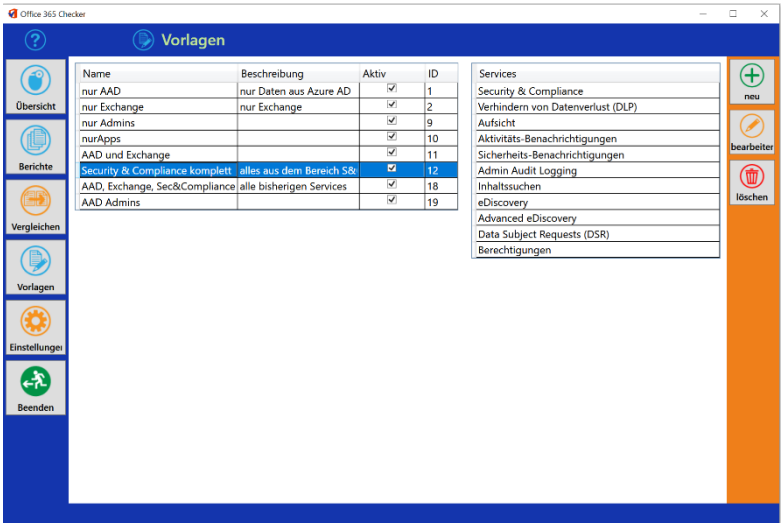
# Vorlagen erstellen

Über Vorlagen steuern Sie, welche Dienstkonfigurationen von Microsoft 365 Sie in einem Bericht zusammenfassen möchten. So können Sie zum Beispiel eine Vorlage erstellen, um die Konfiguration aller genutzten Dienste in einem Bericht zusammenzufassen, Sie können aber auch für jeden einzelnen Dienst wie Exchange, Azure Active Directory, etc. eine eigene Vorlage erstellen. Sie können auch lediglich eine einzelne Funktion in eine Vorlage aufnehmen, um beispielsweise einen eigenen Bericht für das Berechtigungskonzept in Microsoft 365 zu erstellen.

Die Anzahl der Vorlagen ist nicht beschränkt.

Um mit Vorlagen zu arbeiten wählen Sie den Bereich Vorlagen 

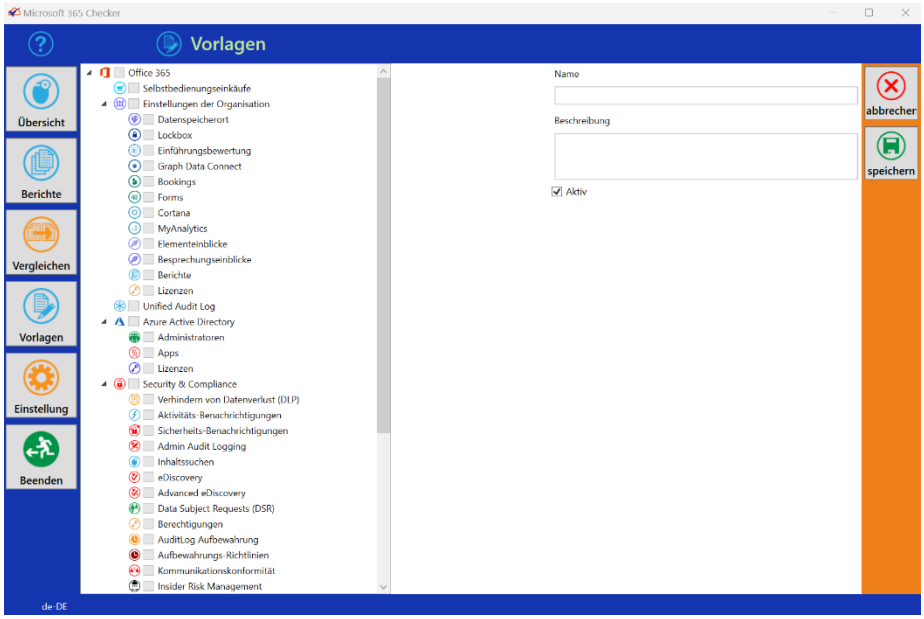

Sie erhalten eine Ansicht der bereits definierten Vorlagen:




Klicken Sie in der Liste auf eine bestehende Vorlage, so wird angezeigt, welche Dienstkonfigurationnen in dieser Vorlage zusammengefasst sind.

## Eine neue Vorlage erstellen

Um eine neue Vorlage zu erstellen, klicken Sie auf den Funktionsschalter „Neu“.




In der Baumstruktur auf der linken Seite werden Ihnen alle Konfigurationen angezeigt, die der Microsoft 365 Checker auslesen kann. Wählen Sie hier die gewünschten Dienste aus, die Sie in einem Bericht zusammenfassen möchten.

Die Bereiche „Selbstbedienungseinkäufe“ und „Einstellungen der Organisation“ sind nur verfügbar, wenn die entsprechenden optionalen PowerShell Module installiert sind.

Geben Sie ihrer Vorlage anschließend einen Namen und eine Beschreibung. Über das Kontrollkästchen „aktiv“ können Sie festlegen, dass diese Vorlage bei der Erstellung eines neuen Berichtes nicht mehr angeboten wird.

Klicken Sie auf „speichern“ um Ihre neue Vorlage zu erstellen.

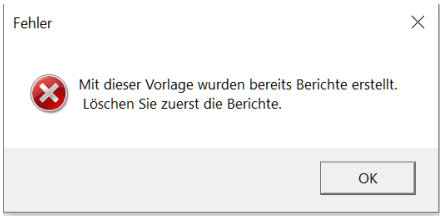
## Vorlagen bearbeiten

Über „Vorlage bearbeiten können Sie den Namen, die Beschreibung und den Status einer Vorlage (aktiv oder inaktiv) ändern. Die einmal in einer Vorlage zusammengefassten Dienste können Sie nicht nachträglich ändern, da ansonsten der Vergleich einzelner Berichte inkonsistent wird.

Um eine Vorlage zu bearbeiten, wählen Sie diese aus der Liste der Vorlagen aus und klicken auf „ändern“.
Nachdem Sie die gewünschten Änderungen durchgeführt haben, klicken Sie auf „speichern“.

## Vorlagen löschen

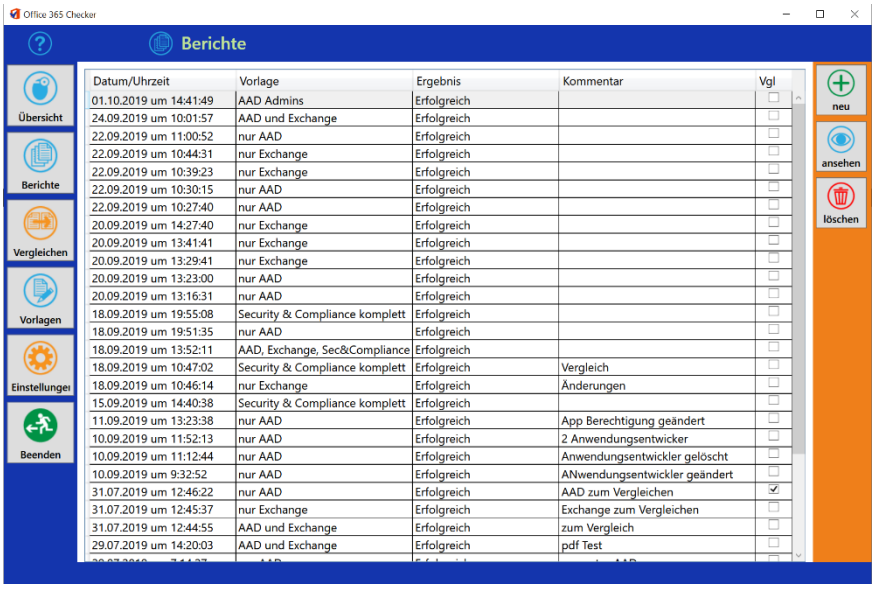
Vorlagen, auf deren Basis noch keine Berichte erstellt worden sind, können Sie wieder löschen. Wählen Sie dazu die zu löschende Vorlage aus der Liste aus und klicken Sie auf „löschen“. Die Vorlage wird gelöscht und verschwindet aus der Liste.
Sind mit der ausgewählten Vorlage bereits Berichte erstellt worden, so erhalten Sie eine entsprechende Meldung:




Sie müssen also zuerst die auf dieser Vorlage basierenden Berichte löschen, bevor Sie die Vorlage löschen können. Das Vorgehen ist unter „Bericht löschen“ beschrieben.

# Berichte erstellen

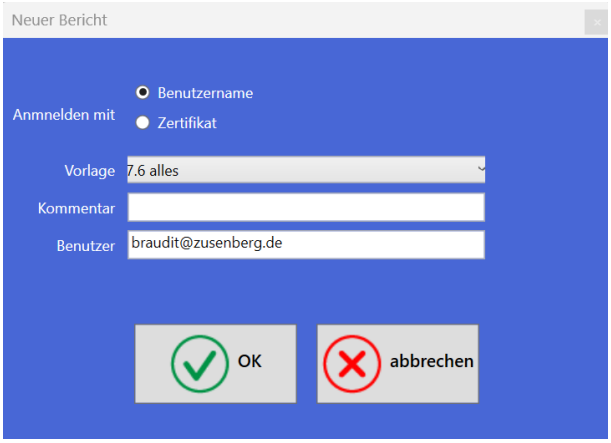
In Berichten werden die aus Microsoft 365 ausgelesenen Konfigurationen zusammengestellt. Um mit Berichten zu arbeiten, klicken Sie auf den Bereich „Berichte“.




Hier sehen Sie nun eine Liste der bereits erstellten Berichte. Angezeigt werden Datum und Uhrzeit der Erstellung sowie den Namen der Vorlage, auf der die Berichte beruhen. In der Spalte „Ergebnis“ sehen Sie, ob der Bericht erfolgreich erstellt werden konnte. Haben Sie bereits Kommentare zu einem Bericht eingetragen, so werden auch diese angezeigt. In der Spalte „Vgl“ können Sie erkennen, welchen Bericht Sie als Vergleichsgrundlage gekennzeichnet haben.

## Neue Berichte erstellen

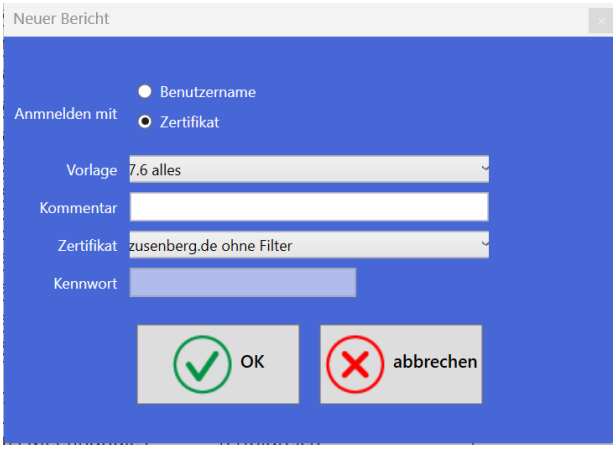
Das Dialogfenster zum Erstellen neuer Berichte hat sich entsprechend der neuen Funktionen geändert:




**Hinweis**:
Vorläufig (voraussichtlich bis Anfang 2025) ist auch der „alte“ Dialog der Checker-Version 7.x noch verfügbar.
Um den alten Dialog zum Erstellen neuer Berichte zu erhalten, drücken Sie die linke Umschalt-Taste (Shift) und klicken dann auf das Plus-Zeichen für einen neuen Bericht.

Bei der Anmeldung mit Benutzernamen wird ab Anfang 2025 ein Konto mit aktivierter Multi-Faktor-Authentifizierung vorausgesetzt. Die Abfrage des Kennwortes erfolgt interaktiv, nachdem Sie auf „OK“ geklickt haben.

Wenn Sie die Anmeldung auf „Zertifikat“ umstellen, ändert sich das Dialogfenster:




In der Liste „Zertifikat“ werden alle erstellten Anmeldedateien aufgelistet (siehe dazu: „Zertifikat-basierte Anmeldung einrichten“)

Wählen Sie die gewünschte Anmeldedatei und geben Sie das dazugehörige Kennwort ein.

Der Checker benutzt dann die in der Anmeldedatei hinterlegten Informationen zum Zertifikat um sich an PowerShell, bzw. am Microsoft Graph anzumelden. Bei der Anmeldung per Zertifikat ist kein Benutzerkonto mehr erforderlich.

Es wird das rotierende Microsoft 365 Checker Logo angezeigt und der Hinweis „Bericht wird erstellt“.

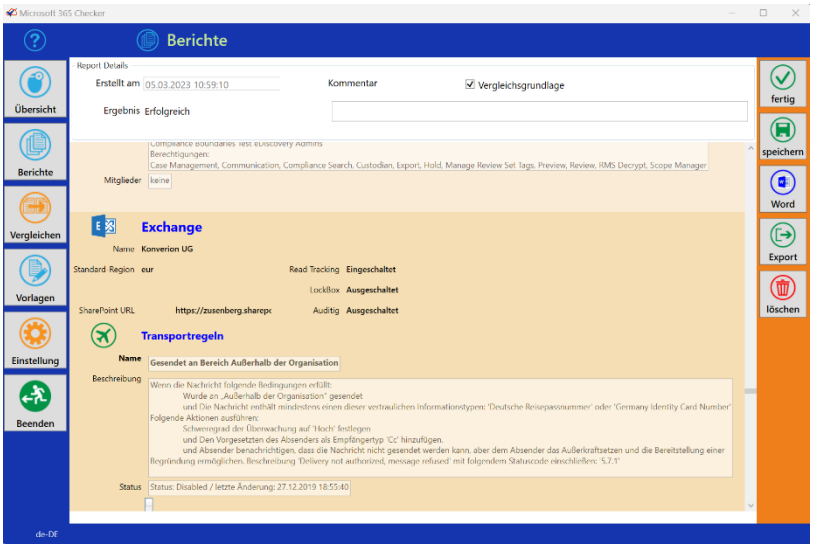
Je nach Menge der zu lesenden Konfigurationen kann die Erstellung eines Berichtes mehrere Minuten bis zu einigen Stunden in Anspruch nehmen.

Ist die Berichterstellung fertig, so wird wieder die Liste der bereits vorhandenen Berichte angezeigt. Der neu erstellte Bericht wird in der obersten Zeile angezeigt.

Um den Bericht anzusehen, wählen Sie den Bericht in der Liste aus und klicken Sie auf „ansehen“.

## Berichte ansehen

Um einen beliebigen Bericht aus Ihrer Liste der vorhandenen Berichte anzusehen, doppelklicken Sie auf den Bericht, oder wählen Sie im Bereich „Berichte“ den gewünschten Bericht aus der Liste aus, und klicken Sie auf „ansehen“.




Im oberen Teil des Anzeigebereiches werden die Details zum Bericht dargestellt. Dies sind Datum und Uhrzeit der Erstellung, der Status, ob der Bericht erfolgreich erstellt werden konnte, der Kommentar zu diesem Bericht sowie das Kontrollkästchen „Vergleichsgrundlage“. Dies ist im Abschnitt „Vergleichsgrundlage festlegen“ erklärt.

Im unteren Teil des Anzeigebereichs sehen Sie den eigentlichen Bericht mit den ausgelesenen Konfigurationen. Was hier genau angezeigt wird hängt davon ab, welche Vorlage Sie zur Erstellung des Berichts gewählt haben. Der generelle Aufbau ist jedoch immer gleich:

Ein Kopfbereich mit den allgemeinen Informationen und dem Icon zum gelesenen Microsoft 365 Dienst (im Bild oben: Exchange). Danach folgen Abschnitte für die gelesenen Konfigurationen (im Bild oben „Transportregeln“), die ebenfalls mit einem Icon gekennzeichnet sind. Innerhalb der Abschnitte dann – abhängig von der gelesenen Konfiguration, ein oder mehrere Paragraphen mit den konkreten Konfigurationen. Im Bild oben für die beiden Transportregeln „Gesendet an Bereich Außerhalb der Organisation“ und „Wissbegierig“.

Mit Hilfe des Scrollbalkens können Sie den gesamten Bericht durchblättern.

## Gefilterte Berichte ansehen

Wenn Sie in der Liste der Berichte einen Bericht auswählen, und dann auf den Schalter 

klicken, wir der anzuzeigende Bericht gefiltert.

In einem gefilterten Bericht werden folgende Informationen ausgeblendet:

- alle nicht genutzten Administratorrolle aus dem Azure Active Directory (Rollen ohne Mitglieder)
- alle im Azure AD registrierten Apps, die keine Anwendungsberechtigungen auf den Microsoft Graph haben
- alle Sicherheitsbenachrichtigungen im Bereich Security & Compliance, die von Microsoft vordefiniert sind
- alle nicht genutzten Berechtigungsrollen aus dem Bereich Compliance (Rollen ohne Mitglieder)
- die „Advanced Rules“ für die Richtlinien zum Verhindern von Datenverlust (DLP)

Die Filterung kann Berichte zum Teil erheblich verkürzen, ohne relevante Informationen für die Mitbestimmung oder den Datenschutz auszulassen.

Wenn Sie einen gefilterten Bericht ansehen, wird in der Kopfzeile das entsprechende Symbol angezeigt.

Wenn Sie einen gefilterten Bericht exportieren oder als Word-Dokument ausgeben lassen, werden auch nur die gefilterten Daten berücksichtigt.

Der Filter entfernt keine Daten aus einem Bericht, sie werden lediglich in dieser Ansicht nicht dargestellt.

## Vergleichsgrundlage festlegen

Wenn Sie nach Durchsicht eines Berichtes festgestellt haben, dass die gelesenen Konfigurationen so sind, wie sie sein sollten – also wie beispielsweise in einer Betriebsvereinbarung festgelegt – können Sie diesen Bericht als Vergleichsgrundlage festlegen, indem Sie das Kontrollkästchen „Vergleichsgrundlage“ aktivieren und anschließend auf „speichern“ klicken.

Dadurch wird dieser Bericht dann im Bereich „Vergleichen“ immer als oberster angezeigt. Näheres hierzu im Abschnitt „Berichte vergleichen“.

## Bericht als Word Dokument speichern

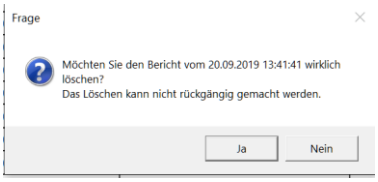
Um einen Bericht als Word Dokument zu speichern, muss Microsoft Word auf dem PC installiert sein. Wählen Sie im Bereich „Berichte“ den gewünschten Bericht aus und klicken Sie anschließend auf „ansehen“. Daraufhin wird Ihnen der gewählte Bericht angezeigt. Klicken Sie auf den Schalter „Word“. Es wird eine Word-Datei aus dem Bericht erstellt und im Ordner „c:\Data\Office365Checker\Berichte“ gespeichert.

Der Dateiname des Berichtes setzt sich aus dem Datum und der Uhrzeit der Erstellung zusammen, also etwa „18-09-2019_13-52-11.docx“ für einen Bericht, der am 18.09.2019 um 13:52.11 Uhr erstellt wurde.

Sie können den Bericht nun in Microsoft Word öffnen und ggf. drucken.

## Bericht löschen

Um einen Bericht zu löschen, wählen Sie im Bereich „Berichte“ den gewünschten Bericht aus und klicken Sie anschließend auf „löschen“. Es erscheint eine Sicherheitsabfrage, ob Sie den gewählten Bericht wirklich löschen wollen:




Einmal gelöschte Berichte können nicht widerhergestellt werden. Bevor Sie also Berichte löschen exportieren Sie ggf. den Bericht oder erstellen Sie eine Datensicherung der Datenbank (siehe „“ im Bereich „Einstellungen“).

Um mehrere Berichte gleichzeitig zu löschen, können Sie durch drücken der Umschalt-Taste Bereiche von Berichte, bzw. durch Drücken der Strg-Taste mehrere einzelne Berichte markieren. Wenn Sie anschließend auf „löschen“ klicken, werden nach einer Sicherheitsabfrage alle markierten Berichte gelöscht.

Sie können einen Bericht auch löschen, wenn Sie in der Berichtsansicht sind. Hier ist ebenfalls ein Schalter „löschen“ vorhanden. Auch hier wird der gewählte Bericht permanent und unwiederbringlich gelöscht.

Eventuell vorhandene Exporte des gelöschten Berichts werden nicht gelöscht.

## Bericht exportieren

Sie können Berichte exportieren, um sie in einer anderen Installation des Microsoft 365 Checkers wieder zu importieren.

Damit können Sie zum Beispiel Berichte durch die IT-Abteilung erstellen, diese exportieren und dem Betriebsrat zur Verfügung stellen. Dieser kann die Berichte nun importieren, ohne dass er dazu ein Konto mit Leseberechtigungen für die Konfiguration von Microsoft 365 benötigt. Die Möglichkeit bietet eine Alternative zur Verwendung des gekapselten Modus.

Um einen Bericht zu exportieren, wählen Sie im Bereich „Berichte“ den gewünschten Bericht aus und klicken Sie anschließend auf „ansehen“. Daraufhin wird Ihnen der gewählte Bericht angezeigt. Klicken Sie auf den Schalter „Export“. Sie erhalten ein Dialogfenster in dem Sie festlegen können, wo die Export-Datei gespeichert wird. Der Standardname ist „Export.tra“. Sie können den Namen beliebig ändern, die Dateiendung „.tra“ wird immer beibehalten.
Die Export-Datei wird automatisch verschlüsselt und mit einer Checksumme versehen, sodass eine Änderung an den exportierten Berichten nicht möglich ist. Jegliche Änderungen an dem Inhalt der exportierten Datei führen dazu, dass sich die Datei nicht wieder importieren lässt.

## Bericht importieren

Um exportierte Berichte zu importieren, klicken Sie im Bereich „Berichte“ auf „Import“. Es erscheint ein Dialogfenster, über welches Sie die zu importierenden Datei (Dateiendung „.tra“) auswählen können. Bestätigen Sie die Auswahl mit „Öffnen“.
Die Datei wird entschlüsselt und mit der enthaltenen Checksumme verglichen. Verläuft die Prüfung erfolgreich, wird der Bericht importiert. Andernfalls erhalten Sie eine Fehlermeldung, dass die Datei beschädigt ist.

Der importierte Bericht wird im Kommentarfeld mit dem Zusatz „[Import]“ versehen.

Zusätzlich zum Bericht wird auch die für die Erstellung des Berichtes genutzte Vorlage installiert. Der ursprüngliche Vorlagenname wird dabei um „[Import]“ ergänzt. War der ursprüngliche Name der Vorlage beispielsweise „Alle Dienste“, so finden Sie ihn nach dem Import in der Liste der Vorlagen unter dem Namen „[Import] Alle Dienste“.

Berichte können nicht in die gleiche Instanz des Microsoft 365 Checkers importiert werden, von der sie exportiert worden sind.

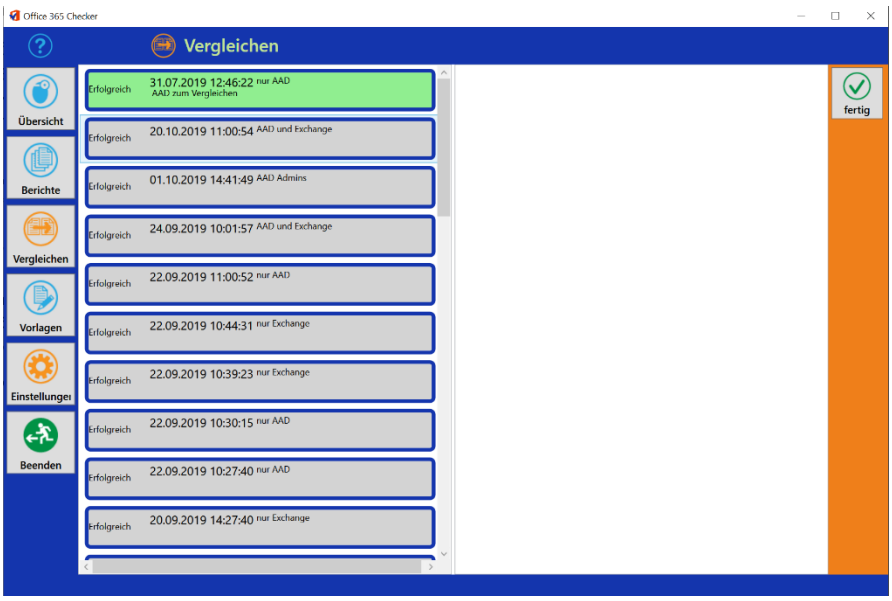
Hinweis:

Wenn Sie importierte Berichte miteinander vergleichen möchten, dann achten Sie darauf, dass die Berichte alle vom gleichen Computer aus exportiert wurden. Jeder Installation des Microsoft 365 Checkers hat eine eigene ID, die zur Unterscheidung der Vorlagen mit exportiert wird. Dadurch wird beim Import mehrerer Berichte, die mit gleicher Vorlage und auf dem gleichen PC erstellt wurden, die entsprechende Vorlage nur einmal installiert, und Sie können diese Berichte miteinander vergleichen.
Stammen die Berichte von unterschiedlichen PCs, so werden die Vorlagen jeweils mit importiert, selbst wenn sie den gleichen Namen haben. Berichte, die auf unterschiedlichen Vorlagen beruhen, können dann nicht miteinander verglichen werden.

# Berichte vergleichen

Um Änderungen in der Konfiguration in Ihrem Microsoft 365 Tenant einfach nachvollziehen zu können, können Sie einmal erstellte Berichte miteinander vergleichen. Im Microsoft 365 Checker werden Ihnen dabei die festgestellten Unterschiede dargestellt.
Sie können nur Berichte miteinander vergleichen, die auf Basis der gleichen Vorlage erstellt wurden.

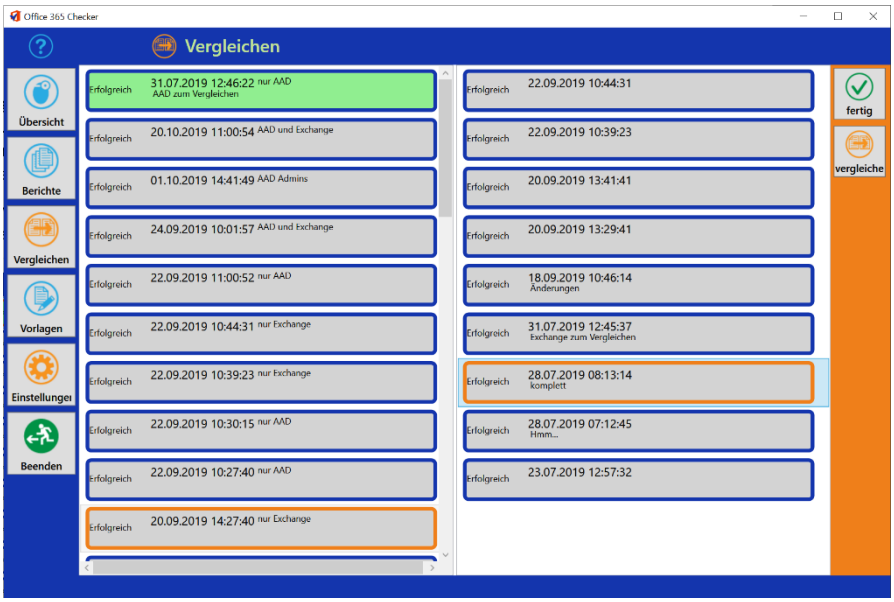
Um Berichte miteinander zu vergleichen wählen Sie den Bereich „Vergleichen“.




Es wird Ihnen eine Liste aller bereits erfolgreich erstellten Berichte angezeigt. Für jeden Bericht sehen Sie Datum und Uhrzeit der Erstellung, die genutzte Vorlage, sowie einen eventuell vorhandenen Kommentar.

Wenn Sie bereits einen Bericht als Vergleichsgrundlage definiert haben, so wird dieser Bericht immer an oberster Stelle in der Liste angezeigt und mit einem grünen Hintergrund versehen. Wählen Sie aus der Liste den Bericht aus, den Sie mit einem anderen vergleichen möchten. Der gewählte Bericht wird mit einem orangenen Rahmen versehen.

Daraufhin werden Ihnen in der rechten Spalte des Anzeigebereiches alle Berichte angezeigt, die auf der gleichen Vorlage basieren, wie der gewählte Bericht.

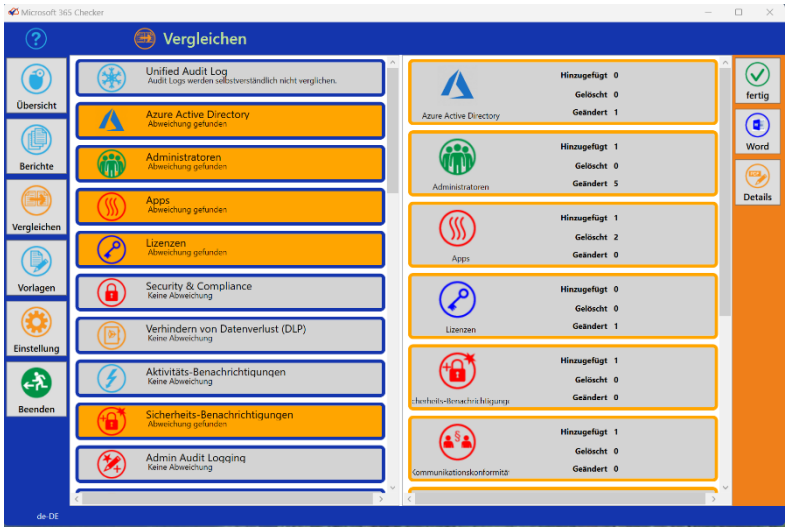



Wählen Sie aus der rechten Liste den Bericht aus, mit dem der orange markierte Bericht der linken Liste verglichen werden soll.

Der gewählte Bericht wird ebenfalls orange umrandet und es erscheint ein Funktionsschalter „vergleichen“.

Klicken Sie nun auf „vergleichen“, um den Vergleich der gewählten Berichte durchzuführen.

Der Microsoft 365 Checker stellt Ihnen nun das Ergebnis des Vergleiches dar:




In der Liste auf der linken Seite werden alle Dienste aufgeführt, deren Konfiguration in den Berichten erfasst worden sind. Wurden bei einem Dienst in den Konfigurationen keine Abweichungen gefunden, so ist der Dienst mit einem grauen Hintergrund und der Bemerkung „keine Abweichung“ dargestellt.

Wurden bei einem Dienst Unterschiede in den beiden verglichenen Berichten erkannt, so erhält der Dienst einen orangenen Hintergrund und die Bemerkung „Abweichung gefunden“.

Für diese Dienste werden dann die gefundenen Abweichungen jeweils in der rechten Spalte angezeigt.

Beispiele:


Es wurde eine Informationen im Bereich „Azure Active Directory geändert.

Es wurde eine neue Rolle im Azure Active Directory hinzugefügt und es gab 5 Änderungen an bestehenden Rollen.

Es wurde eine neu App im Azure Active Directory registriert und 2 Apps gelöscht.

## Detailvergleich

Mit einem Klick auf den Schalter „Details“ wird ein PDF-Dokument mit den konkreten Änderungen erstellt und im Ordner „c:\data\office365checker\Berichte“ gespeichert. Voraussetzung ist, dass Microsoft Word auf dem PC installiert ist.
Diesem Bericht sind die konkreten Änderungen zu entnehmen.

Azure Active Directory

```
Geändert: AAD_Info userCount =>
Alt:
390
Neu:
391
```

Bei obigem Beispiel:
Es wurde ein Benutzer neu angelegt, daher hat sich der Benutzerzähler (userCount) von 390 auf 391 erhöht.

Administratoren


```
Hinzugefügt: [
 "displayName": "Power Platform Administrator",
 "description": "Can create and manage all aspects of Microsoft Dynamics 365, PowerApps and Microsoft Flow.",
 "objectId": "02621d17-5be3-4db4-b6f9-af3a4d627c76",
 "members": [
  {
   "displayName": "100117",
   "givenName": "",
   "surname": "",
   "email": "100117@zusenberg.de"
  },
  {
   "displayName": "100113",
   "givenName": "",
   "surname": "",
   "email": "100113@zusenberg.de"
  }
 ]
```


Die administrative Rolle „Power Platform Administrator“ mit den beiden Benutzern 100117@zusenberg.de und 100113@zusenberg.de wurde neu erstellt.

```
Geändert: "displayName": "User Administrator" =>
Gelöscht:
{
  "displayName": "Bernd Nordberg",
  "givenName": "Bernd",
  "surname": "Nordberg",
  "email": "Bernd.Nordberg@zusenberg.de"
}
Geändert: "displayName": "User Administrator" =>
Hinzugefügt:
{
  "displayName": "Gerd Geis",
  "givenName": "Gerd",
  "surname": "Geis",
  "email": "Gerd.Geis@zusenberg.de"
}
Geändert: "displayName": "User Administrator" =>
Hinzugefügt:
{
  "displayName": "Lisa Brummel",
  "givenName": "Lisa",
  "surname": "Brummel",
  "email": "lisa.brummel@zusenberg.de"
}
```

Die administrative Rolle „User Administrator“ wurde geändert.
„Bernd.Nordberg@zusenberg.de“ wurde aus der Rolle gelöscht, „Gerd.Geis@zusenberg.de“ und „Lisa.Brummel@zusenberg.de“ wurden neu hinzugefügt.

## Übersicht des Vergleichs in Word exportieren

Über der Funktionsschalter „Word“ kann eine Zusammenfassung der Ergebnisse des Vergleichs in einer Word-Datei gespeichert werden. Voraussetzung ist, dass Microsoft Word auf dem PC installiert ist.
Wie auch Berichte werden die Word-Dateien der Vergleiche im Ordner „c:\Data\Microsoft365Checker\Berichte“ gespeichert. Der Dateiname ist „Vergleich_ *Datum&Uhrzeit*“, also beispielsweise „Vergleich_24-09-2019_13-55-20.docx“ für einen Vergleich, der am 24.09.2019 um 13:55.20 Uhr gespeichert wurde.

# Einstellungen

Die Kategorie „Einstellungen ist in sechs Bereiche unterteilt, die nachfolgend beschrieben werden.

## Allgemein

In diesem Bereich können Sie den Standardbenutzer hinterlegen, der beim Erstellen eines neuen Berichtes automatisch in die Eingabemaske übernommen wird.

Wenn Sie hier Änderungen vornehmen nicht vergessen auf „speichern“ zu klicken. Ansonsten werden die Änderungen verworfen.

Im Bereich „Ergebnisse einschränken“ können Sie festlegen, dass

a) personenbezogene Daten von Benutzern nur dann angezeigt werden, wenn diese Benutzer einem bestimmten Land, einer Firma, oder einer Nutzungsregion zugeordnet sind, und
b) nicht die Namen der Administratoren, sondern nur die Gesamtzahl pro Rolle im Bericht genannt werden

Im Bereich „Gekapselter Modus“ (nur noch verfügbar bis Anfang 2025) können Sie die Verschlüsselungsdatei für den gekapselten Modus erstellen, wie im Abschnitt „Erstellen der Office365Checker.o3c Datei“ beschrieben.

Mit der Einstellung „Proxy Einstellungen benutzen (beta)“ könne Sie festlegen, dass der Microsoft 365 Checker zur Verbindung mit dem Internet die für den Internet Explorer definierten Proxy-Einstellungen verwendet. Die Funktion ist noch im Beta-Stadium und nicht vollständig getestet. Treten bei Verwendung dieser Funktion Probleme auf, so wenden Sie sich an support@konverion.de.

Mit dem Kontrollkästchen „Konto mit Multi-Faktor-Authentifizierung (MFA)“ können Sie die Unterstützung von MFA-gesicherten Konten einschalten. Mit eingeschalteter MFA-Unterstützung kann es vorkommen, dass sie sich zur Erstellung eines Berichtes mehrfach anmelden müssen. Außerdem schließen sich MFA und gekapselter Modus gegenseitig aus, da MFA immer ein interaktives Login erfordert. Daher werden die Einstellungen für den gekapselten Modus ausgeblendet, sobald Sie MFA aktivieren.

Ab Anfang 2025 ist die Anmeldung ohne MFA für Benutzerkonten mit administrativen Berechtigungen nicht mehr möglich.

Im Bereich „Info“ erhalten Sie Informationen zur aktuellen Versionsnummer des Programmes sowie der Datenbank. Diese Informationen werden eventuell im Supportfall von Ihnen abgefragt.

## Daten

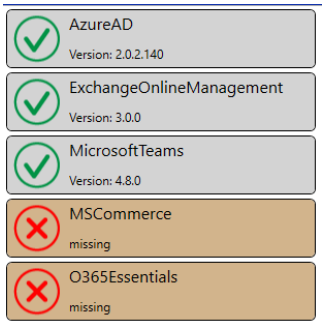
Hier sehen Sie den aktuellen Pfad zur Datenbank (Office365Checker.db3). Bei Bedarf können Sie die Datenbank über den Schalter „verschieben“ auf eine andere Festplatte oder in ein anderes Verzeichnis verschieben. Solange keine gewichtigen Gründe vorliegen, sollten Sie die Datenbank jedoch dort belassen, wo sie ist.

Über „ändern“ können Sie die gewählte Datenbank ändern, zum Beispiel um auf eine zuvor gesicherte Datenbank (siehe Datensicherung) zuzugreifen.

Über den Schalter „sichern“ können Sie eine Sicherungskopie Ihrer Datenbank anlegen. Klicken Sie den Schalter an, so erscheint ein Dialogfenster mit dem Sie festlegen können, wo die Sicherungskopie abgelegt werden soll. Der Namensvorschlag für die Sicherungskopie ist Office365Checker_*Datum&Uhrzeit*.sdf, wobei *Datum&Uhrzeit* das aktuelle Datum und die Uhrzeit der Sicherung sind. Sie können den Namen beliebig ändern.

## PS (PowerShell)

In diesem Bereich erhalten Sie einen Überblick, welche PowerShell Module für den Microsoft 365 Checker installiert sind.




Hier sind die Module

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

installiert.
Die optionalen Module „MSCommerce“ und „O365Essentials“ sind nicht installiert.

Sie können der Liste ebenfalls die aktuell installierte Version des jeweiligen PowerShell Moduls entnehmen.

Um ein Modul zu installieren, oder die aktuellste Version zu installieren, klicken Sie auf das entsprechende Modul. Nach einer Sicherheitsabfrage wird das gewählte Modul dann auf Ihren PC kopiert, und im Ordner „c:\data\office365checker\PS“ abgelegt.

Für die Erstinstallation von PowerShell Modulen sind administrative Rechte auf Ihrem lokalen PC notwendig.

## Microsoft Graph

Ab der Version 8 des Checker kann anstelle der PowerShell Module „AzureAD“, AzureAD Preview“ und „MSCommerce“ die Microsoft Graph Programmierschnittstelle (API) für das Auslesen der entsprechenden Konfigurationen genutzt werden.
Die Nutzung des Microsoft Graph bringt im Wesentlichen 3 Vorteile:

- der Microsofft Graph wird ständig weiterentwickelt,
- der Microsoft Graph unterstützt moderne Authentifizierung, und
- das Auslesen der Konfigurationen ist erheblich schneller (etwa Faktor 5)

Der Nachteil ist, dass man für die Nutzung des Microsoft Graph und der Zertifikat-basierten Anmeldung in Entra ID eine Anwendung registrieren muss, um den Checker mit den notwendigen Berechtigungen auszustatten.
Dafür wird kein Konto mit „Global Reader“ Berechtigungen mehr benötigt. Es wird gar kein Benutzerkonto mehr benötigt, da die Authentifizierung / Autorisierung über die registrierte Anwendung erfolgt.
Bedauerlicherweise ist es zumindest derzeit noch nicht möglich, alle Dienste auf den Microsoft Graph umzustellen. Insbesondere das Exchange Modul (zum Auslesen der Exchange und Compliance Einstellungen), sowie das Teams Modul können noch nicht ersetzt werden, da Microsoft die dafür notwendigen Funktionen (Rest-API Endpunkte) noch nicht verfügbar gemacht hat.

### Anwendung in Entra ID registrieren

Zum Registrieren von Anwendungen müssen Sie mindestens die Rolle „Anwendungsadministrator“ besitzen.
Öffnen Sie dazu das Entra ID Admin Center (https://entra.microsoft.com/) und erweitern in der linken Menüleiste den Bereich „Anwendungen“.

Klicken Sie anschließend auf „App Registrierungen“. Sie sehen nun eine Liste der bereits in Ihrem Tenant registrierten Anwendungen.

Klicken Sie auf „Neue Registrierung“.
Vergeben Sie einen Namen für die Anwendung (zum Beispiel „Microsoft 365 Checker“) und lassen Sie alle weiteren Einstellungen so wie sie sind. Klicken Sie auf „Registrieren“.

Damit ist die Anwendung registriert und der Bildschirm sollte so aussehen:


Öffnen Sie nun den Windows Editor (oder ein beliebiges anderes Textverarbeitungprogramm) und kopieren Sie die auf dieser Seite angezeigte „Anwendungs-ID (Client)“ und die „Verzeichnis-ID (Mandant). Diese werden später für die Konfiguration des Checkers benötigt.

Als nächstes müssen in der Anwendung die erforderlichen Berechtigungen eingestellt werden.
Klicken Sie hierzu auf „API-Berechtigungen“.
Standardmäßig ist für den Microsoft Graph die Berechtigung „User.Read“ vom Typ „Delegiert[1]“ eingetragen.

Klicken Sie nun auf „Berechtigung hinzufügen“, und aus der Liste der häufig verwendeten Microsof-APIs auf „Microsoft Graph“.

Bei der Art der Berechtigungen wählen Sie „Anwendungsberechtigungen“. Sie erhalten jetzt eine Liste mit allen möglichen Berechtigungen (mehr als 800).

Öffnen Sie den Bereich „Application“ und markieren „Application.Read.All“.

Scrollen Sie zum Bereich „Directory“ und markieren „Directory.Read.All“.

Scollen Sie zum Bereich „RoleManagement“ und markieren Sie „RoleManagement.Read.Exchange“.

Scrollen Sie zum Bereich „RoleManagementPolicy“ und markieren „RoleManagementPolicy.Read.Directory“.

Bestätigen Sie mit „Berechtigung hinzufügen“.

Klicken Sie anschließend auf erneut „Berechtigungen hinzufügen“.

[1] Zum Unterschied zwischen den Berechtigungstypen „Delegiert“ und „Anwendung“ siehe Abschnitt „Berechtigungstypen“,

Klicken Sie erneut auf „Berechtigungen hinzufügen“ und dann auf „Von meiner Organisation verwendete APIs“.
Tragen Sie in der Suchzeile „M365“ ein.

Wählen Sie aus der Liste „M365 License Manager“.
Im Bereich „Delegierte Berechtigungen“ wählen Sie „LicenseManager.AccessAsUser“.
Klicken Sie auf „Anwendungsberechtigungen“ und aktivieren „LicensedProduct.Read.All“.

Bestätigen Sie mit „Berechtigungen hinzufügen“.

Hinweis: Der „LicenseManager“ dient zum Auslesen der Einstellungen zu den Selbstbedienungs-Einkäufen. Derzeit kann auf den LicenseManager nur im „Delegierten Modus“ zugegriffen werden. Bei Zertifikat-basierter Anmeldung können diese Einstellungen nicht ausgelesen werden.

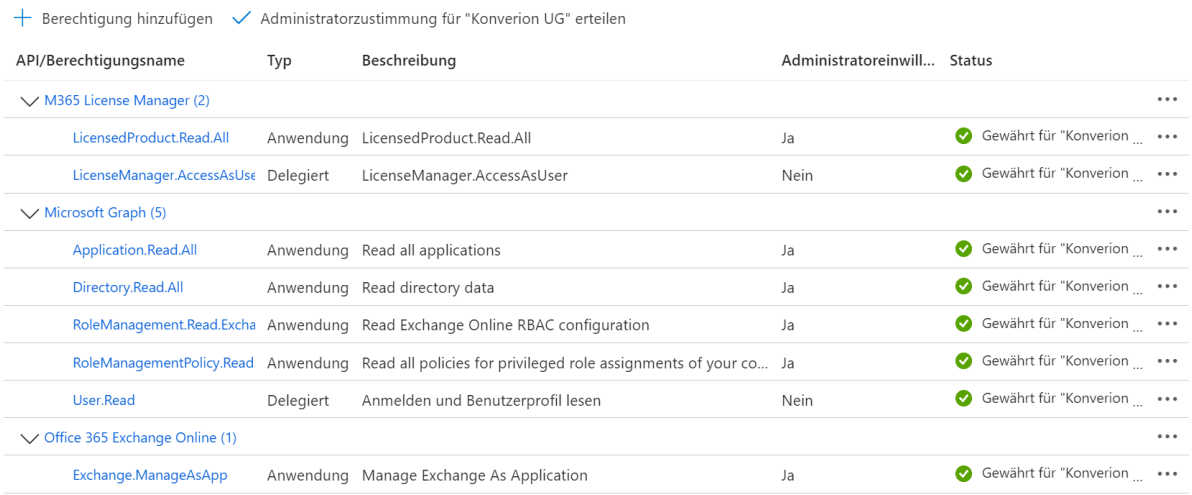
Klicken Sie erneut auf „Berechtigungen hinzufügen“ und dann auf „Von meiner Organisation verwendete APIs“.
Tragen Sie in der Suchzeile „Office“ ein.

Wählen Sie aus der Liste „Office 365 Exchange Online“.
Klicken Sie auf „Anwendungsberechtigungen“ und aktivieren Sie im Bereich „Exchange“ „Exchange.ManageAsApp“.

Bestätigen Sie mit „Berechtigungen hinzufügen“.

Um die Anforderungen zu genehmigen klicken Sie auf „Administratorzustimmung für [Ihre Organisation] erteilen“ und bestätigen anschließend mit „Ja“. Der Status der Berechtigungen ändert sich damit in „Gewährt für [Ihre Organisation]“.

Die Liste der konfigurierten Berechtigungen sollte nun so aussehen:

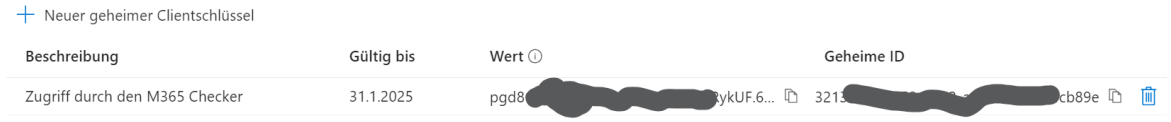



| API/Berechtigungsname | Typ | Beschreibung | Administratoreinwill... | Status |
|---|---|---|---|---|
| M365 License Manager (2) | | | | |
| LicensedProduct.Read.All | Anwendung | LicensedProduct.Read.All | Ja | Gewährt für "Konverion ... |
| LicenseManager.AccessAsUse | Delegiert | LicenseManager.AccessAsUser | Nein | Gewährt für "Konverion ... |
| Microsoft Graph (5) | | | | |
| Application.Read.All | Anwendung | Read all applications | Ja | Gewährt für "Konverion ... |
| Directory.Read.All | Anwendung | Read directory data | Ja | Gewährt für "Konverion ... |
| RoleManagement.Read.Excha | Anwendung | Read Exchange Online RBAC configuration | Ja | Gewährt für "Konverion ... |
| RoleManagementPolicy.Read | Anwendung | Read all policies for privileged role assignments of your co... | Ja | Gewährt für "Konverion ... |
| User.Read | Delegiert | Anmelden und Benutzerprofil lesen | Nein | Gewährt für "Konverion ... |
| Office 365 Exchange Online (1) | | | | |
| Exchange.ManageAsApp | Anwendung | Manage Exchange As Application | Ja | Gewährt für "Konverion ... |

Abschließend muss noch der Zugriff konfiguriert werden.
Klicken Sie dazu auf „Zertifikate & Geheimnisse“. Im Bereich „Geheime Clientschlüssel“ klicken Sie auf „+ Neuer geheimer Clientschlüssel“.
Es öffnet sich ein Dialogfenster, in dem Sie eine Beschreibung des Schlüssels und eine Gültigkeitsdauer festlegen können. Tragen Sie als Beschreibung „Zugriff durch den M365 Checker“ ein und wählen Sie eine Gültigkeitsdauer.
Hinweis: nach Ablauf der Gültigkeitsdauer müssen Sie eine neuen Clientschlüssel generieren und den

Checker entsprechend neu konfigurieren. Die Gültigkeitsdauer kann nachträglich nicht verlängert werden.

Die Anzeige sollte jetzt so aussehen:




WICHTIG: Kopieren Sie jetzt den Wert (nicht die Geheime ID) in die oben erstellte Datei mit der Verzeichnis ID und der Client ID.

Damit ist die Registrierung der Anwendung abgeschlossen.
Sie haben folgende Berechtigungen vergeben:

| Bereich | Berechtigung | Zweck |
|---|---|---|
| Microsoft Graph | Application.Read.All | Alle registrierten Anwendungen in Entra ID auslesen |
| Microsoft Graph | Directory.Read.All | Benutzer und Gruppen auslesen (erforderlich zum Auslesen der Administratoren, um Namen und Gruppen auflösen zu können) |
| Microsoft Graph | RoleManagementPolicy.Read.Directory | Rollenzuweisungen für das Priviledged Identity Management auslesen |
| Microsoft Graph | RoleManagement.Read.Exchange | Auslesen der Purview-Rollen |
| M365 License Manager | LicensedProduct.Read.All | Einstellungen für Selbstbedienungseinkäufe auslesen |
| M365 License Manager | LicenseManager.AccessAsUser | Als Benutzer am Lizenz-Manager anmelden |
| Exchange | Exchange.ManageAsApp | Der Anwendung Zugriff auf die Exchange und Compliance Konfiguration gewähren. |

## Berechtigungstypen

Bei der Vergabe von Berechtigungen für den Zugriff auf Programmierschnittstellen (APIs) im Rahmen der Anwendungsregistrierung unterscheidet man zwischen den Typen „Delegiert“ und „Anwendung“.

„Delegiert“ bedeutet, die Anwendung, die auf Daten über die Programmierschnittstelle zugreifen möchte, tut dies im Namen des Benutzers, also auch genau mit den Berechtigungen, die dieser Benutzer bereits hat. Über delegierte Berechtigungen werden also keine weiteren Berechtigungen vergeben, sondern lediglich festgelegt, über welche APIs welche der bestehenden Berechtigungen eines Benutzers genutzt werden können.
Wenn Sie also beispielsweise einer Anwendung die delegierte Berechtigung „Mail.Read“ für den Microsoft Graph erteilen, kann ein angemeldeter Benutzer seine E-Mails auch über den Microsoft Graph lesen (zusätzlich zu Outlook, Outlook im Web, etc.).

Beim Typ „Anwendung“ erhält die Anwendung an sich Berechtigungen, unabhängig vom angemeldeten Benutzer – oder auch ganz ohne angemeldeten Benutzer.

Wenn Sie also einer Anwendung die Berechtigung „Mail.Read.All“ auf den Microsoft Graph geben, kann diese Anwendung über den Microsoft Graph alle E-Mails sämtlicher Benutzer in Ihrem Tenant lesen. Unabhängig davon, wer diese Anwendung gerade benutzt.
Solche weitreichenden Berechtigungen sind zum Beispiel für Anwendungen erforderlich, die eine Datensicherung Ihrer Dateien oder E-Mails erstellen sollen.

## Microsoft 365 Checker für Graph konfigurieren

Nach dem Start des Checkers wechseln Sie zu „Einstellungen“ und „Graph“.
Tragen Sie in das Feld „Tenat ID“ die Verzeichnis ID ein, in das Feld „Client ID“ die Anwendungs-ID und in das Feld „Client Secret“ den Wert, den Sie beim Erstellen des Anwendungsgeheimnisses kopiert haben.

Klicken Sie auf „Anmeldung testen“.

In der Ausgabe sollte dann

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

erscheinen, wobei „displayName“ und „city“ den Wert Ihrer Organisation enthalten.

Bei erfolgreicher Anmeldung wird „Graph benutzen, wenn möglich“ aktiviert.
Wenn Sie den nächsten Bericht erstellen, der Einstellungen aus Entra ID oder die Selbstbedienungseinkäufe ausliest, wird dazu der Microsoft Graph und nicht mehr ein PowerShell Modul genutzt.
Sie können diese Funktion bis Ende März 2025 (Einstellung der AzureAD PowerShell Module) jederzeit wieder ausschalten, um den Graph nicht weiter zu benutzen und die Einstellungen wieder per PowerShell auszulesen.
Zum erneuten Einschalten klicken Sie wieder auf „Anmeldung testen“.

## Zertifikat-basierte Anmeldung einrichten

Mit der Zertifikat-basierten Anmeldung kann der Checker benutzt werden, ohne dass ein spezielles Benutzerkonto erforderlich ist.
Einschränkung:
Die optionalen PowerShell Module „MSCommerce“ und „O365Essentials“ unterstützen keine Zertifikat-basierte Anmeldung. Die entsprechenden Einstellungen können also bei der Nutzung von Zertifikaten (zumindest derzeit) nicht ausgelesen werden.

Es können sowohl „offizielle“, als auch selbst-signierte Zertifikate genutzt werden.

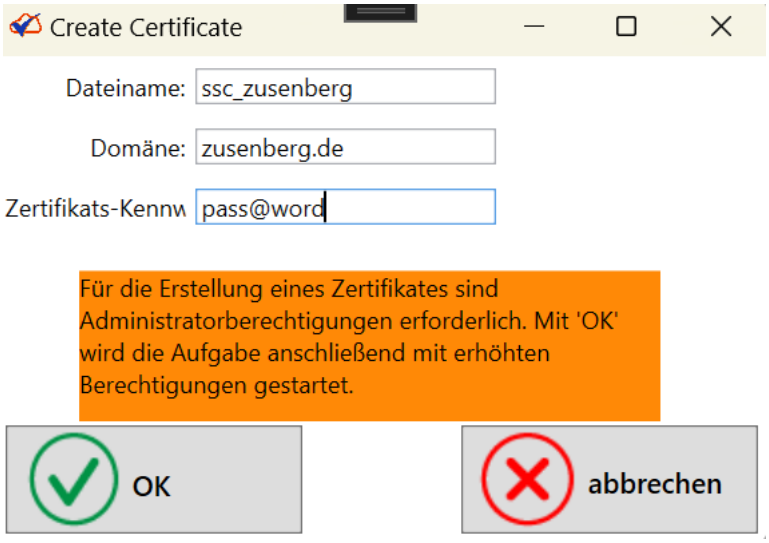
Um die Zertifikat-basierte Anmeldung zu nutzen sind vier Schritte erforderlich:

1) Erstellen eines selbst-signierten Zertifikates, bzw. Export der entsprechenden Zertifikats-Dateien aus Ihrer eigenen PKI
2) Registrieren des Zertifikats in der Entra ID App
3) Erteilen der notwendigen Berechtigungen
4) Erstellen einer Anmeldedatei

### *Schritt 1 – Zertifikat erstellen*

Um ein selbst-signiertes Zertifikat zu erstellen, gehen Sie wie folgt vor:
Öffnen Sie den Microsoft 365 Checker und wechseln Sie zu „Einstellungen“ Cert“.
Klicken Sie auf „Zertifikat erstellen“.

In dem nun angezeigten Fenster geben Sie den Dateinamen für das Zertifikat, die Domäne, sowie ein Kennwort zur Verschlüsselung des privaten Schlüssels an.
Beispiel:




Hinweis: Das Kennwort darf kein „#“ enthalten.

Da die Erstellung und Signierung des Zertifikates nur mit Administratorberechtigungen erfolgen kann, erscheint nach Klicken auf „OK“ der entsprechende Dialog der Benutzerkontensteuerung, der die Zustimmung zur Erteilung erhöhter Berechtigungen an das Programm „MakeCert.exe“ (Bestandteil des Microsoft 365 Checkers) anfordert.
Bei Bestätigung mit „Ja“ wird ein Zertifikat, sowie der dazugehörige private Schlüssel erstellt.

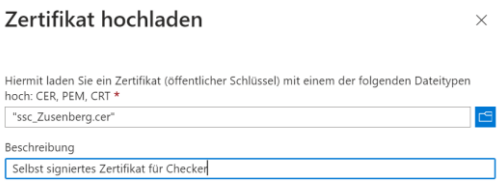
Die Dateien finden Sie im Verzeichnis „C:\data\office365checker\certs“. Bei Verwendung des oben benutzen Dateinamens finden Sie in diesem Verzeichnis nun die Dateien „ssc_Zusenberg.cer“ (Zertifikatdatei) sowie „ssc_Zusenberg.pfx“ (Privater Schlüssel).

Das Zertifikat wird ebenfalls in Ihrem Zertifikatsspeicher auf der lokalen Maschine gespeichert. Sie finden es im Zertifikats-Manager (Certmgr.exe) unter „Eigene Zertifikate“. Dieses Zertifikat wird nicht genutzt und kann gelöscht werden.

### *Schritt 2 – Zertifikat in der registrierten App importieren*

Im nächsten Schritt importieren Sie das Zertifikat in die bereits in Entra ID registrierte App.

Im Entra ID Admin-Portal öffnen Sie die entsprechende App (im Beispiel: „Microsoft 365 Checker“) und wählen Sie „Zertifikate & Geheimnisse“. Gehen Sie hier auf die Registerkarte „Zertifikate“.
Wählen Sie „Zertifikat hochladen“.
Wählen Sie die soeben erstellte Zertifikats-Datei (im Beispiel: „ssc_Zusenberg.cer“) aus und geben Sie eine Beschreibung ein.



Bestätigen Sie mit „Hinzufügen“.
Das hinzugefügte Zertifikat wird in der Liste der Zertifikate angezeigt.

### *Schritt 3 - Erteilen der notwendigen Berechtigungen*

Wenn sich der Checker mit einem Zertifikat authentisiert erfolgt dies über den ServicePrincipal der registrierten App. Daher muss der ServicerPrincipal über ausreichende Berechtigungen verfügen, um die Konfigurationen auslesen zu dürfen.

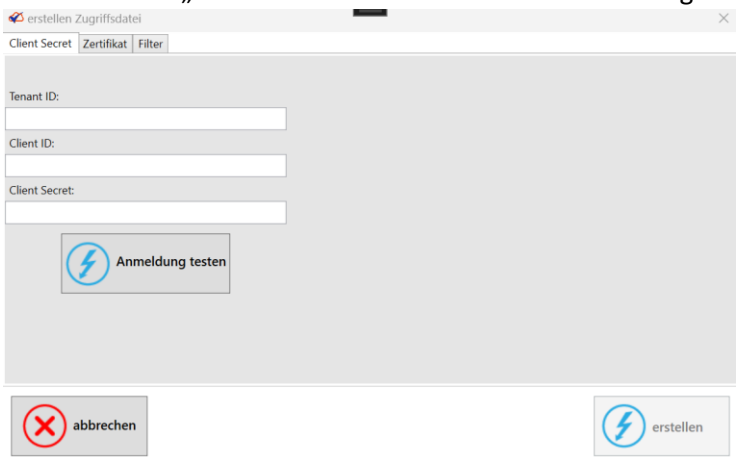
Wählen Sie im Entra ID Admin Center den Bereich „Rollen und Administratoren“ und suchen Sie nach der Rolle „Globaler Leser“ und wählen diese aus. Klicken Sie auf „Zuweisungen hinzufügen“ und tragen Sie im Suchfeld den Namen der von Ihnen registrierten App ein, wählen Sie diese aus und klicken Sie auf „Hinzufügen“.

Der ServicePrincipal der App wird jetzt in der Liste der Zuweisungen angezeigt.

### *Schritt 4 – Anmeldedatei erstellen*

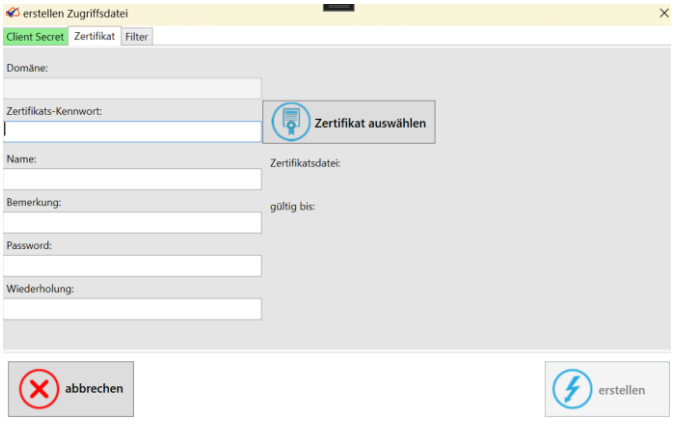
Über die Anmeldedatei wird der Ersatz für den „gekapselten Modus“ erreicht. Sie können also sicherstellen, das eine Nutzung der Zertifikates nur durch den Checker erfolgen kann. Außerdem können Sie Einschränkungen für die zu erstellenden Berichte festlegen.
Dazu wird das Kennwort für den privaten Schlüssel, sowie ggf. die gewählten Einschränkungen, mit einem von Ihnen zu vergebenden Kennwort in der Anmeldedatei verschlüsselt gespeichert.

Wenn also Ihr Betriebsrat den Checker früher im „gekapselten Modus“ genutzt hat, um Berichte selbst zu erstellen, können Sie dies nun durch die Zertifikat-basierte Anmeldung ersetzen.
Dazu geben Sie die Datei mit dem persönlichen Schlüssel (*.pfx), die Anmeldedatei (*.o3s), sowie das Kennwort für die Anmeldedatei an den Betriebsrat.
Dazu müssen die beiden Dateien im Verzeichnis „c:\data\office365checker\certs“ abgelegt werden.
Vorgehensweise:
Gehen Sie im Microsoft 365 Checker auf „Einstellungen“ und „Cert“.
Klicken Sie auf „Anmeldedatei erstellen“. Es erscheint folgendes Fenster:




Tragen Sie hier die Tenant ID, Client ID und Client Secret wie im Abschnitt „Anwendung in Entra ID registrieren“ beschrieben ein. Klicken Sie anschließend auf „Anmeldung testen“. Ist die Anmeldung erfolgreich, färbt sich der Hintergrund grün.

Wechseln Sie anschließend auf die Kartei „Zertifikat“:




Tragen Sie zuerst das Kennwort für den privaten Schlüssel ein, welches Sie beim Erstellen des Zertifikates vergeben haben. Klicken Sie anschließend auf „Zertifikat auswählen“ und wählen sie den erstellten privaten Schlüssel (*.pfx Datei) aus.
Daraufhin wird der Pfad zur Zertifikatsdatei, das Gültigkeitsdatum, sowie der Domänenname ausgelesen und angezeigt.

Vergeben Sie nun einen Namen für die zu erstellende Anmeldedatei, eine Beschreibung, sowie ein Kennwort zur Verschlüsselung der Anmeldedatei.

Bei Bedarf können Sie nun noch Einschränkungen festlegen.
Wechseln Sie dazu auf die Karteikarte „Filter“. Hier können Sie festlegen, dass in den Berichten nur personenbezogene Daten von Benutzern aus einem bestimmten Land (Feld=Country), einer bestimmten Firma (Feld=CompanyName), oder einem bestimmten Datenspeicherort (Feld= UsageLocation) ausgelesen werden ausgelesen werden können.
Außerdem können Sie festlegen, dass nur die Anzahl der Administratoren in den jeweiligen Rollen, aber nicht deren Namen ausgelesen werden können.

Klicken Sie abschließend auf „erstellen“.

Im Verzeichnis „c:\data\office365checker\certs“ wird eine Datei mit dem von Ihnen vorgegebenen Namen und der Endung „.o3s“ erstellt. Dies ist die Anmeldedatei.

In den Zertifikatseinstellungen sehen Sie die neu erstellte Anmeldedatei in der Liste. Sie können beliebig viele Anmeldedateien – zum Beispiel mit unterschiedlichen Filtereinstellungen – erstellen.

### Lizenz

Im Bereich „Lizenz“ wird Ihnen der Status Ihrer Lizenz angezeigt. Hier sehen Sie den Typ Ihrer Lizenz („Demo“ oder „general“) und wie lange Ihre Lizenz noch gültig ist.

Bei lizensierten Versionen wird hier ebenfalls angezeigt, für welche Domäne(n) der Microsoft 365 Checker lizensiert ist.

## Übersicht

Im Bereich „Übersicht“ wird derzeit die Anzahl der Vorlagen und erstellten Berichte angezeigt.

# Veraltete Funktionen nutzen (Checker Version 7.x)

Bis Microsoft die angekündigten Änderungen technisch umsetzt, können die „alten“ Funktionen des Checkers weiter genutzt werden.
Bis Anfang 2025 ist also noch eine Anmeldung ohne MFA möglich und bis zum 30. März 2025 können die Azure AD PowerShell Module noch genutzt werden.

## Gekapselter Modus

Wie im Abschnitt „Vorbereitung“ dargestellt, benötigt man für den Einsatz des Microsoft 365 Checkers ein Benutzerkonto, welches Leseberechtigung für möglichst alle Einstellungen im Microsoft 365 Tenant hat. Dies ist am einfachsten über die Rolle „Global Reader“ zu erreichen. Für den Zugriff auf die AuditLogs benötigt das Konto zusätzlich die Rolle „Sicherheitsleseberechtigter“.
Insbesondere in größeren Unternehmen bestehen jedoch häufig Bedenken, dem Betriebsrat ein Konto mit derart weitreichenden Leserechten zur Verfügung zu stellen, da hiermit ja zum Beispiel auch die Konfiguration (nicht die Inhalte!) der Konten von Führungskräften eingesehen werden könnte.

Um hier eine für beide Seiten tragfähige Lösung zur Verfügung zu stellen, wurde im Microsoft 365 Checker ein „gekapselter Modus“ integriert. In diesem Modus kann das Benutzerkonto mit den notwendigen Berechtigung ausschließlich in Verbindung mit dem Microsoft 365 Checker eingesetzt werden. Ein direkter Zugriff über das Konto auf den Microsoft 365 Tenant ist damit nicht mehr möglich.
So können auf der einen Seite die Informationsansprüche des Betriebsrates, auf der anderen Seite aber auch die Sicherheitsansprüche der IT befriedigt werden.

Für internationale Unternehmen oder Unternehmen mit mehreren Betriebsräten kann die Anzeige von personenbezogenen Daten in den Berichten eingeschränkt werden. Damit sieht dann jeder Betriebsrat nur noch personenbezogenen Daten von den Mitarbeitern, die auch durch ihn vertreten werden.

Die Vorgehensweise hierzu ist im Abschnitt „Gekapselten Modus verwenden“ beschrieben.

## Multi-Faktor-Authentifizierung

Ab der Version 5.4 ist die Unterstützung von Konten mit Multi-Faktor-Authentifizierung (MFA) für die Nutzung des Microsoft 365 Checkers möglich.

Generell sei noch darauf hingewiesen, dass sich MFA und gekapselter Modus gegenseitig ausschließen, da für MFA immer ein interaktives Login erforderlich ist.

Deshalb kann man seit der Version 5.4 des Checkers die Filteroptionen auch unabhängig vom gekapselten Modus nutzen.

So können bei eingeschalteter Multi-Faktor-Authentifizierung Berichte durch die IT passend für jedes Betriebsratsgremium erstellt und exportiert werden. Da exportierte Berichte verschlüsselt und mit einer gehashten Checksumme versehen sind, ist eine Manipulation der Exporte nicht möglich.

Wie Sie den gekapselten Modus verwenden könne, ohne auf die Sicherheit eines zweiten Faktors verzichten zu müssen, lesen Sie im folgenden Abschnitt.

## Richtlinien für bedingten Zugriff

Da sich der gekapselte Modus und Multi-Faktor-Authentifizierung technisch gegenseitig ausschließen, bieten sich Richtlinien für den bedingten Zugriff (Conditional Access Policies) als Lösung an.
Damit können die interaktiven Standard-MFA Verfahren durch einen „statischen“ zweiten Faktor

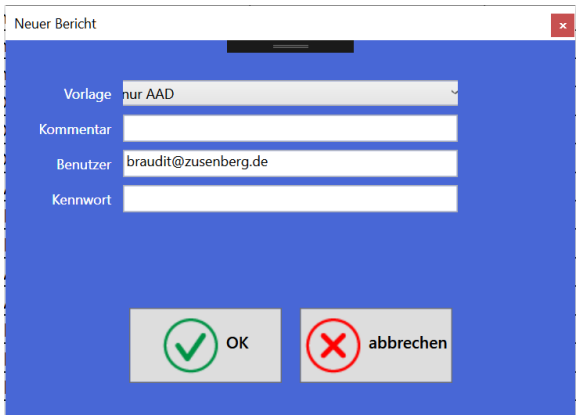
ersetzt werden. Je nach eingesetzter Technologie können so als zweiter Faktor z.B. erlaubte IP-Adressen / -Bereiche oder auch im Azure AD registrierte Geräte dienen.

Um also auch den gekapselten Modus mit einem zweiten Authentifizierungsfaktor nutzen zu können, deaktivieren Sie für das Konto, das für die Betriebsrats-Kontrollen vorgesehen ist, die Multi-Faktor Authentifizierung.
Anschließend erstellen Sie eine Richtlinie für bedingten Zugriff, die für dieses Konto die Anmeldung nur von definierten IP-Adressen erlaubt.

Weiterführende Informationen, wie man MFA für einzelne Benutzerkonten deaktiviert und Richtlinien für den bedingten Zugriff erstellt finden Sie hier : https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa

## Einen neuen Bericht erstellen

Um einen neuen Bericht über die Dialogfenster der Version 7.x des Checkers zu erstellen, halten Sie die linke Umschalt-Taste (Shift) gedrückt und klicken Sie dann auf den Funktionsschalter „+neu“. Daraufhin erscheint ein Dialogfenster.



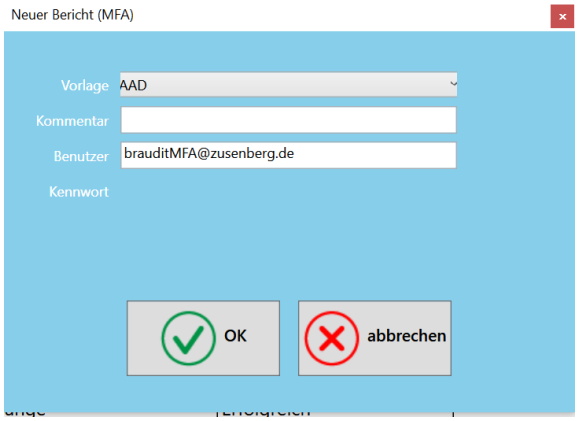

Klicken Sie auf das Auswahlfeld „Vorlage“, so wird Ihnen eine Liste aller bereits definierten Vorlagen angezeigt, die den Status „aktiv“ haben. Wählen Sie hier die gewünschte Vorlage aus, auf deren Basis Sie einen Bericht erstellen wollen. Sie können bereits jetzt einen Kommentar zu dem noch nicht erstellten Bericht eingeben. Dies kann aber auch nach Erstellung des Berichtes erfolgen.

Als nächstes müssen Sie ein Benutzerkonto sowie das dazugehörige Kennwort eingeben, mit dem sich der Microsoft 365 Checker an Ihrem Microsoft 365 Tenant anmelden soll. Um einen Bericht erfolgreich erstellen zu können, muss das angegebene Konto über Leseberechtigungen für die in der gewählten Vorlage zusammengestellten Dienste verfügen. Sinnvoll ist der Einsatz eines Kontos mit der Berechtigung „Global Reader“ in Microsoft 365.

Den Benutzernamen können Sie in den Einstellungen des Microsoft 365 Checkers voreinstellen. Das Kennwort wird nie gespeichert.

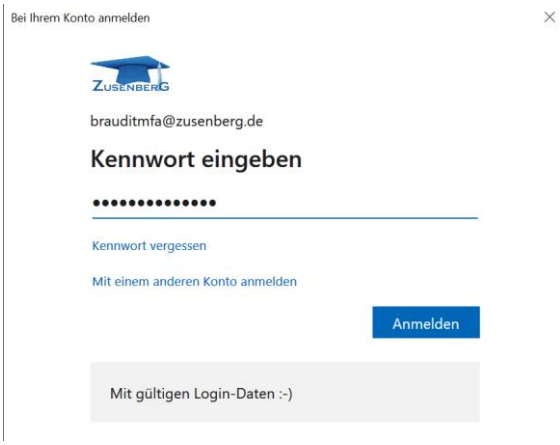
Klicken Sie auf „OK“, und der Microsoft 365 Checker beginnt mit der Erstellung des Berichtes.

Wenn Sie die Multi-Faktor Authentifizierung benutzen, hat das Dialogfenster ein etwas anderes aussehen:

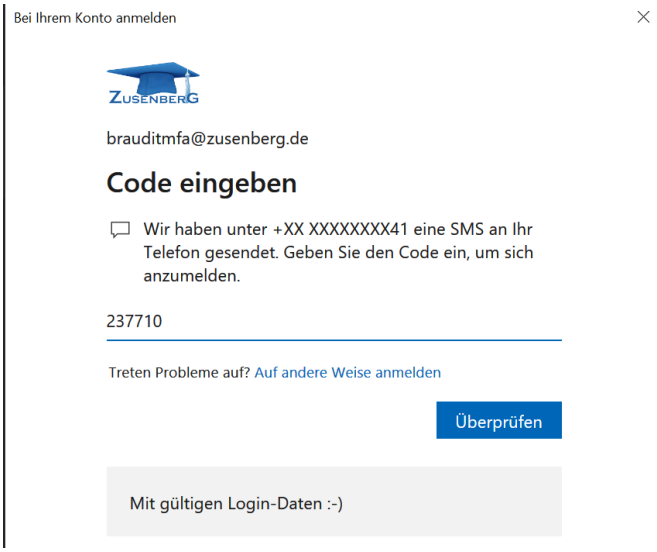



MFA erfordert immer ein interaktives Login, sodass in dem Dialogfenster kein Kennwort eingetragen werden kann.

Wenn Sie mit „OK“ bestätigen erhalten Sie den interaktiven Dialog zur Anmeldung




Nach Eingabe des Kennwortes und klicken auf „Anmelden“ erhalten Sie als nächstes die MFA-Aufforderung. Je nach Einstellung im Unternehmen per SMS Code, Authenticator App,…




Nach klicken auf „Überprüfen“ (oder Bestätigung durch die Authenticator App) startet die Berichtserstellung.

Es wird das rotierende Microsoft 365 Checker Logo angezeigt und der Hinweis „Bericht wird erstellt“.

Je nach Menge der zu lesenden Konfigurationen kann die Erstellung eines Berichtes mehrere Minuten bis zu einigen Stunden in Anspruch nehmen.

Ist die Berichterstellung fertig, so wird wieder die Liste der bereits vorhandenen Berichte angezeigt. Der neu erstellte Bericht wird in der obersten Zeile angezeigt.

Um den Bericht anzusehen, wählen Sie den Bericht in der Liste aus und klicken Sie auf „ansehen“.

## Gekapselten Modus verwenden

Hinweis:
Da Microsoft für alle Benutzerkonten mit administrativen Berechtigungen ab Anfang 2025 Multi-Faktor-Authentifizierung (MFA) erzwingt, und sich MFA und gekapselter Modus gegenseitig ausschließen, wird dieser Modus nur noch bis Angang 2025 unterstützt.
Die Funktionalität des gekapselten Modus wird durch die Zertifikat-basierte Anmeldung ersetzt, die ab der Version 8 des Checkers verfügbar ist.

Mit dem gekapselten Modus wird die Verwendung des Benutzerkontos, welches mit den Leseberechtigungen für die Konfiguration des Tenants ausgestattet ist, auf den Microsoft 365 Checker beschränkt.

Normalerweise erhält der Betriebsrat zur Ausübung seiner Kontrollrechte ein Konto mit der Berechtigung „Global Reader“ eingerichtet (Beispiel: braudit@zusenberg.de).
Mit diesem Konto ist auch eine Anmeldung an den verschiedenen Microsoft 365 Admin Centern möglich, sodass auch ein Zugriff auf die Konfiguration der Konten von Führungskräften möglich wäre.

Im gekapselten Modus wird dieses Konto genauso eingerichtet, jedoch erhält der Betriebsrat nicht mehr das Kennwort für dieses Konto, sondern eine verschlüsselte Datei, sowie ein Verschlüsselungs-Kennwort, mit dem der Microsoft 365 Checker die Datei entschlüsseln kann.

Diese Vorgehensweise funktioniert technisch bedingt nur mit Konten, für die keine Multi-Faktor-Authentifizierung (MFA) eingeschaltet ist. MFA erfordert immer ein interaktives Login.

Die Datei an sich (Office365Checker.o3c) ist verschlüsselt und enthält den Hashwert des Benutzernamens sowie das dazugehörige Kennwort. Selbst wenn diese Datei in „falsche Hände“ geriete und entschlüsselt werden könnte, wäre das Konto nicht kompromittiert, da der Benutzername lediglich als Hashwert gespeichert ist.

Im gekapselten Modus benötigt der Betriebsrat also für den Einsatz des Microsoft 365 Checkers

- den Namen des Benutzerkontos,
- die Datei „Office365Checker.o3c“, sowie
- das Kennwort, um diese Datei zu verwenden.

Es besteht also keine Möglichkeit mehr, sich mit diesem Konto direkt an Microsoft 365 anzumelden.

Um diesen Modus zu verwenden, gehen Sie wie folgt vor:

1. Die IT erstellt das Benutzerkonto
   (im Beispiel: braudit@zuenberg.de mit Kennwort „!streng9Geheim“)

2. Die IT erstellt mit Hilfe des Microsoft 365 Checkers die Datei „Office365Checker.o3c“ mit dem Verschlüsselungskennwort „#IT.verschlüsselt!“
3. Der Betriebsrat erhält:
    a. den Benutzernamen „braudit@zusenberg.de“
    b. die Datei „Office365Checker.o3c“
    c. das Verschlüsselungskennwort „#IT.verschlüsselt!“
4. Der Betriebsrat speichert die Datei im Verzeichnis „c:\data\Office365Checker“.
5. Beim Erstellen eines neuen Berichtes erkennt der Microsoft 365 Checker die Datei und fordert zur Eingabe des Benutzernamens und des Verschlüsselungskennwortes auf.
6. Mit dem Verschlüsselungskennwort wird die Datei entschlüsselt und das Benutzerkennwort „!streng9Geheim“ ausgelesen. Außerdem überprüft das Programm, ob der eingegebene Benutzername dem als Hashwert in der Datei gespeicherten Benutzernamen entspricht.
7. Der Microsoft 365 Checker meldet sich mit dem Konto braudit@zuenberg.de und Kennwort „!streng9Geheim“ an Microsoft 365 an und erstellt die gewünschten Berichte.

Idealer Weise nicht alles in einer Email! 😊

## Einschränken der Ergebnisse

Sie können die Anzeige von personenbezogenen Daten (Name, Email-Adresse,..) in den Berichten einschränken. Dies bezieht sich insbesondere auf die Exchange-Funktionalitäten „Beweissicherung“ und „Journal“, da diese explizit für bestimmte Benutzer angewendet werden.
Dies ist zum Beispiel sinnvoll, um in einem internationalen Unternehmen nur die Daten von deutschen Benutzern in den Berichten aufzunehmen, da ja nur diese durch den Betriebsrat vertreten werden. Auch wenn mehrere deutsche Unternehmen in einem gemeinsamen Tenant zusammengefasst sind, aber unterschiedliche Betriebsräte haben, können Sie durch die Einschränkung erreichen, dass jeder Betriebsrat nur die Daten der von ihm vertretenen Mitarbeitern sieht.

Diese Einschränkungen können auf den Feldern „Firmenname“ (CompanyName), „Land oder Region“ (Country) oder „Nutzungsspeicherort“ (UsageLocation) beruhen.

Beispiel:
Im Tenant eines internationalen Unternehmens ist bei allen Benutzern im Attribut „Land oder Region“ entsprechend dem jeweiligen Sitz des Mitarbeiters mit der Länderkennung ausgefüllt. Bei allen in Deutschland ansässigen also mit „DE“.
Erstellen sie nun eine „Office365Checker.o3c“ Datei mit der Einschränkung „Country=DE“, so werden in den Berichten unter den Punkten „Journal“ oder „Beweissicherungen“ nur noch Benutzernamen von deutschen Mitarbeitern angezeigt. Bei allen anderen erscheint „anonymisiert“:

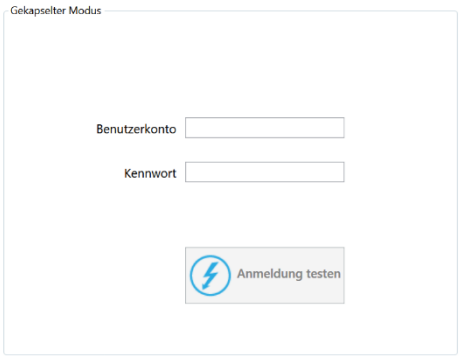

Der erste Benutzer ist also nicht in Deutschland ansässig, „Julia Huber“ schon.

Die Email-Adresse des Administrators, der die entsprechende Konfiguration vorgenommen hat, wird in jedem Fall angezeigt um ggf. Nachfragen stellen zu können.

Des Weiteren können Sie festlegen, dass bei den Berechtigungen nur noch die Anzahl der der jeweiligen Rolle zugeordneten Administratoren ausgelesen wird, aber nicht mehr die konkreten Namen.

## Erstellen der „Office365Checker.o3c“ Datei

Um die Datei „Office365Checker.locked“ zu erstellen, wechseln Sie in den Bereich „Einstellungen“.




Im Bereich „Gekapselter Modus“ geben Sie den Benutzernamen (im Beispiel: braudit@zusenberg.de“ und das dazugehörige Kennwort (im Beispiel: „!streng9Geheim“) ein. Klicken Sie auf den Schalter „Anmeldung testen“. Der Microsoft 365 Checker testet daraufhin die Anmeldung an Ihrem Microsoft 365 Tenant mit den angegebenen Informationen. War die Anmeldung erfolgreich erscheint ein Eingabefeld für das Verschlüsselungskennwort und der Schalter ändert sich in „Datei erstellen“.

Wenn Sie das Kontrollkästchen „Ergebnisse einschränken“ markiert haben, werden die festgelegten Einschränkungen mit in der „Office365Checker.o3c“ Datei verschlüsselt, und können daher vom späteren Benutzer nicht geändert werden.

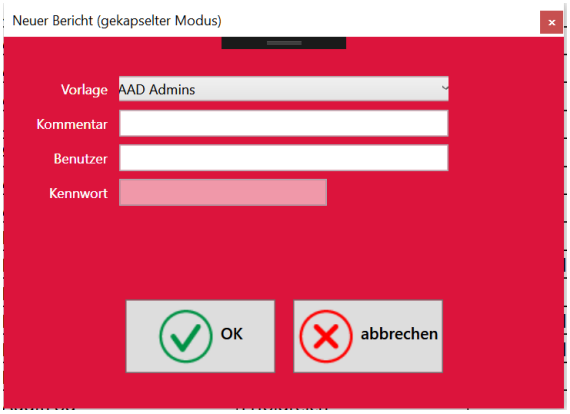
Geben Sie das Verschlüsselungskennwort (im Beispiel: „#IT.verschlüsselt!“) ein und klicken Sie auf „Datei erstellen“.
Achtung: das Verschlüsselungskennwort wird im Klartext angezeigt, bis die Datei gespeichert ist.
Es erscheint ein Dialogfenster in dem Sie auswählen können, wo die Datei gespeichert werden soll.

Nun können Sie die gespeicherte Datei dem Betriebsrat zur Verfügung stellen. Dieser legt sie im Ordner „C:\data\Office365Checker“ auf dem Computer ab, auf dem der Microsoft 365 Checker laufen soll.

Teilen Sie dem Betriebsrat ebenfalls den Benutzernamen sowie das Verschlüsselungskennwort mit.

## Berichte im gekapselten Modus erstellen

Klicken Sie auf den Bereich „Berichte“, halten Sie die linke Umschalt-Taste (Shift) gedrückt und klicken Sie dann auf den Schalter „+Neu“.




Wenn die Datei „Office365Checker.o3c“ im Verzeichnis „C:\data\Office365Checker“ vorhanden ist, wird ein spezielles Dialogfenster zur Erstellung von Berichten im gekapselten Modus dargestellt.

Wählen Sie die Vorlage für den gewünschten Bericht.

Geben Sie anschließend den Benutzernamen (im Beispiel: „braudit@zusenberg.de“) und das Verschlüsselungskennwort (im Beispiel: „#IT.verschlüsselt!“) ein.

Klicken Sie auf OK, und der Bericht wird erstellt.

## Den gekapselten Modus mit einem zweiten Authentifizierungs-Faktor absichern

Da die Multi-Faktor-Authentifizierung immer ein interaktives Anmelden erfordert, können Benutzerkonten, für die MFA eingeschaltet ist, nicht für den gekapselten Modus verwendet werden.

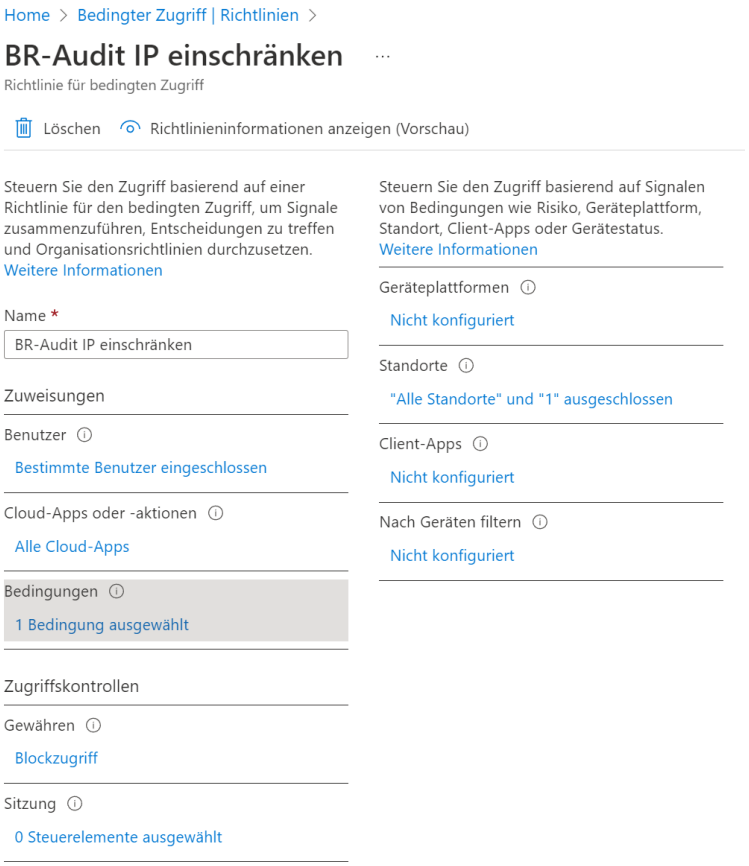
Um auch im gekapselten Modus von der erhöhten Sicherheit eines zweiten Authentifizierungsfaktors Gebrauch machen zu können, ist der Einsatz von „Richtlinien für den bedingten Zugriff“ (Conditional Access Policies) empfehlenswert.
Damit können Sie als zweiten Faktor z.B. eine bestimmte IP-Adresse )/-bereich, oder auch einen registrierten PC (setzt den Einsatz von Microsoft Intune voraus) erfordern.

Gehen Sie dazu wie folgt vor (Beispiel für Einschränkung auf eine bestimmte IP-Adresse):
Legen Sie das gewünschte Benutzerkonto (im Beispiel „braudit-ip@zusenberg.de“) an, und ordnen Sie ihm die Rollen „Globaler Leser und „Sicherheitsleseberechtigter“ zu.

Achten Sie darauf, dass für dieses Konto MFA nicht eingeschaltet ist (ggf. müssen Sie eine Ausnahme in Ihre Richtlinien für bedingten Zugriff eintragen).
Legen Sie im Azure Active Directory im Bereich „Bedingter Zugriff“ einen benannten Standort an. Hier können Sie die IP-Adresse oder den IP-Bereich angeben, von dem aus sich das Konto anmelden kann. So können Sie z.B. sicherstellen, dass eine Anmeldung nur aus dem Unternehmensnetzwerk möglich ist.

Erstellen Sie als nächstes eine neue Richtlinie für bedingten Zugriff.
Als Benutzer tragen Sie das BR-Kontrollkonto ein.
Unter „Cloud Apps und Aktionen“ wählen Sie „Alle Cloud-Apps“.
Bei „Bedingung“ tragen Sie unter „Standorte“ bei „Einschließen“ „Alle Standorte“ ein, und bei „Ausschließen“ den Standort, den Sie soeben angelegt haben.
Unter „Gewähren“ tragen Sie „Blockzugriff“ ein.
Schalten Sie „Richtlinie aktivieren“ auf „Ein“ (oder „Nur Bericht“, wenn Sie es erst testen wollen).

Die Richtlinie sollte nun in etwa so aussehen:




Klicken Sie auf „speichern“.

Wenn Sie die Richtlinie testen möchten, klicken Sie die entsprechende Richtlinie an und wählen aus der oberen Menüleiste „WhatIf“.
Hier können Sie durch Angabe verschiedener Benutzernamen / IP-Adressen testen, wann und wie sich die Richtlinie auswirkt.

Nachdem die neue Richtlinie aktiviert wurde, kann der Microsoft 365 Checker mit dem eingetragene Benutzerkonto nur noch von der festgelegten IP-Adresse aus verwendet werden.

# Problembehandlung

## Der Microsoft 365 Checker lässt sich nicht installieren

Wenn Sie den Microsoft 365 Checker heruntergeladen haben, und nach einem Doppelklick auf die Datei eine Fehlermeldung bekommen, liegt das in den meisten Fällen daran, dass der „Microsoft App-Installer“ auf dem PC nicht vorhanden ist.

Sie können den App-Installer aus dem Microsoft Store kostenlos installieren.
https://www.microsoft.com/store/productId/9NBLGGH4NNS1

Falls Sie den Microsoft Store nicht öffnen können, setzten Sie in der Registry folgenden Wert auf 0:
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStoreRequirePrivateStoreOnly=0

## Installation der PowerShell Module

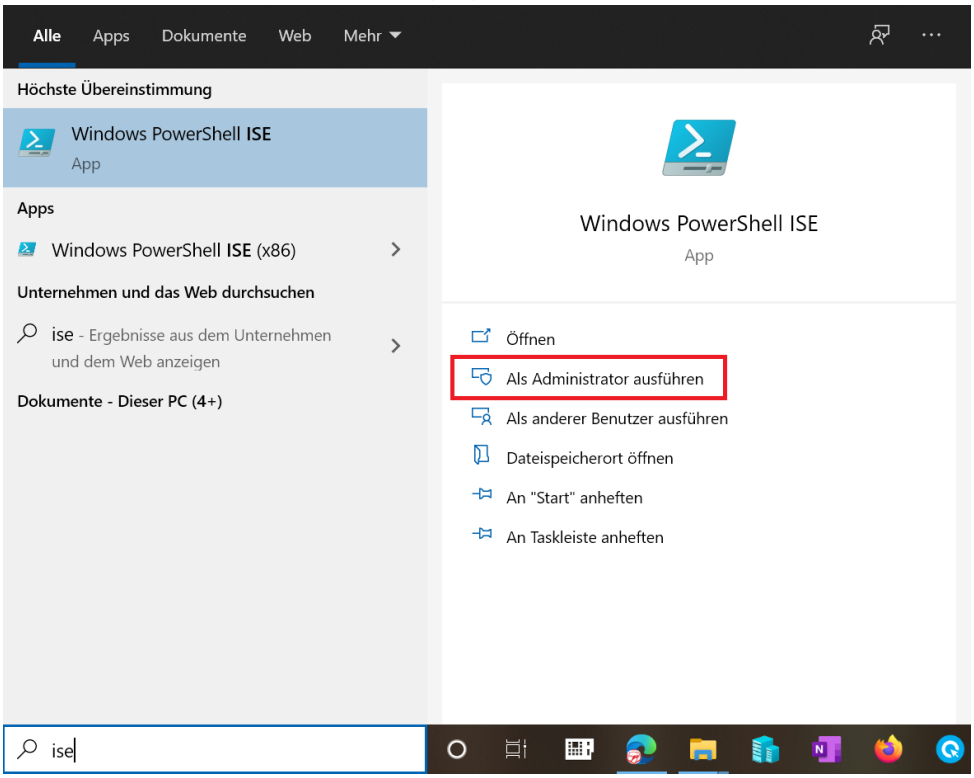
Das häufigste Problem im Umgang mit dem Microsoft 365 Checker tritt auf, wenn die Installation der PowerShell Module nicht ordnungsgemäß funktioniert.

Das hat fast immer folgenden Grund:
Um die benötigten PowerShell Module finden und installieren zu können, wird zuallererst der NuGet Paket Manager benötigt. Um den Paket Manager zu installieren, benötigen Sie Admin-Rechte auf der lokalen Maschine **und** das Ausführen von Scripts für den aktuellen Benutzer muss erlaubt sein.

Wenn eine der beiden Voraussetzungen nicht erfüllt ist, schlägt die Installation fehl, und es können auch keine weiteren PowerShell Module geladen werden.

Sollte das bei Ihnen der Fall sein, gehen Sie wie folgt vor:

Starten Sie die PowerShell-Konsole (ISE) als Administrator

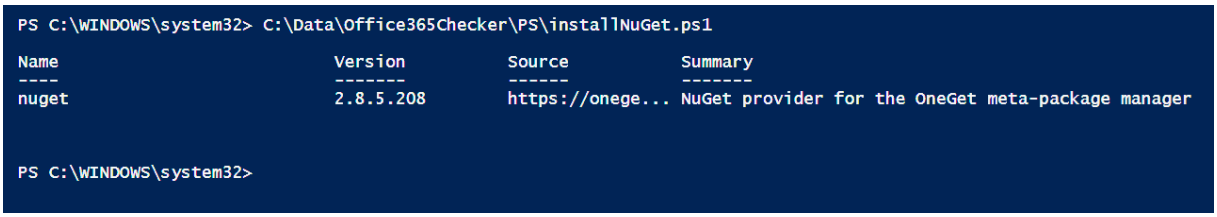



Geben Sie folgenden Befehl ein:

Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser -Force

Führen Sie den Befehl aus. Öffnen Sie anschließend die Datei „c:\data\Microsoft365Checker\PS\installNuGet.ps1“ und führen Sie diese aus.

Nach Beendigung des Scripts sollte die Anzeige so aussehen:




Jetzt können Sie die weiteren PowerShell Module über „Einstellungen – PS“ im Microsoft 365 Checker installieren.

Dazu werden keine administrativen Rechte mehr benötigt.

## Security & Compliance Einstellungen werden nicht gelesen

Wenn nur die Einstellungen aus dem Bereich „Security & Compliance“ nicht gelesen werden können liegt das in aller Regel daran, dass Basic Authentifizierung für WinRM auf dem lokalen PC nicht erlaubt ist.

Öffnen Sie die Eingabeaufforderung und geben Sie folgenden Befehl ein:

```
winrm set winrm/config/client/auth @{Basic="true"}
```

Danach sollten sich auch die Einstellungen aus dem Bereich „Security & Compliance“ auslesen lassen. Ab der Version 3.2 des Exchange PowerShell Moduls sind diese Einstellung nicht mehr nötig sein, weil dann auch die Einstellungen des Compliance Centers per REST_API ausgelesen werden (was für Exchange bereits seit der Version 3.0 des Moduls funktioniert).

Sollten andere Probleme bei Ihnen auftauchen, so öffnen Sie die Datei „log.txt“ mit einem Texteditor. In ihr sind alle Fehlermeldungen des Microsoft 365 Checker festgehalten. Dadurch können Sie unter anderem feststellen, wenn das von Ihnen zum Auslesen der Konfiguration verwendete Konto nicht über ausreichende Berechtigungen verfügt.

Sollten Sie eventuelle Probleme nicht selbst lösen können, so wenden Sie sich an support@konverion.de. Wir setzen und dann umgehend mit Ihnen in Verbindung.

# Anhang: Auslesbare Einstellungen

## Unified Audit Log

Aus dem Unified Audit Log werden die Ereignisse der folgenden Kategorien ausgelesen:

eDiscovery
Advanced eDiscovery
Einstellungen zum Anonymisieren von Verwendungsberichten
Benutzer zu einer Rolle hinzugefügt (zum Administrator gemacht)
Benutzer aus einer Rolle entfernt (Administrator-Rechte entzogen)
WorkplaceAnalytics

Um die Berichte übersichtlich zu halten, werden die durchgeführten Aktionen für eDiscovery, Advanced eDiscovery und Workplace Analytics in Kategorien zusammengefasst und die Gesamtzahl der Aktionen pro Kategorie festgehalten.
Die Erklärungen zu der Bedeutung von „Operations“ finden Sie hier: https://docs.microsoft.com/de-de/microsoft-365/compliance/search-for-ediscovery-activities-in-the-audit-log?view=o365-worldwide
Die Änderungen an den Einstellungen zur Anonymisierung der Verwendungsberichte, sowie zum Hinzufügen und Entfernen von Administratorrolle zu Benutzer und Gruppen werden einzeln aufgeführt.

Beispiel Verwendungsberichte

**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}] |

Bedeutung:
Am 11.02.2022 um 08:40 Uhr wurde die Anonymisierung der Verwendungsberichte vom Benutzer „joergsc@zusenberg.de“ ausgeschaltet, am gleichen Tag um 22:44 Uhr wurde sie wieder eingeschaltet.

Beispiel Vergabe von Administrator-Berechtigungen:

**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 |

Am 11.02.2022 um 11:18 Uhr wurde dem Benutzer brauditttest@zusenberg.de die Rolle „User Account Administrator“ vom Benutzer joergsc@zusenberg.de zugewiesen.

Beispiel Entzug von Administrator-Berechtigungen:

**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 |

Am 11.02.2022 um 11:14 Uhr wurde dem Benutzer brauditttest@zusenberg.de die Rolle „Global Reader“ vom Benutzer joergsc@zusenberg.de entzogen.

## Azure Active Directory

### Info

Name des Tenants
Adresse (Strasse, PLZ, Ort)
Land
Telefon
Privacy Kontakt
URL
Anzahl Benutzer

### AAD Rollen

Sämtliche Rollen mit:
Name
Beschreibung
Rolleninhaber mit Namen, Vornamen und Email-Adresse

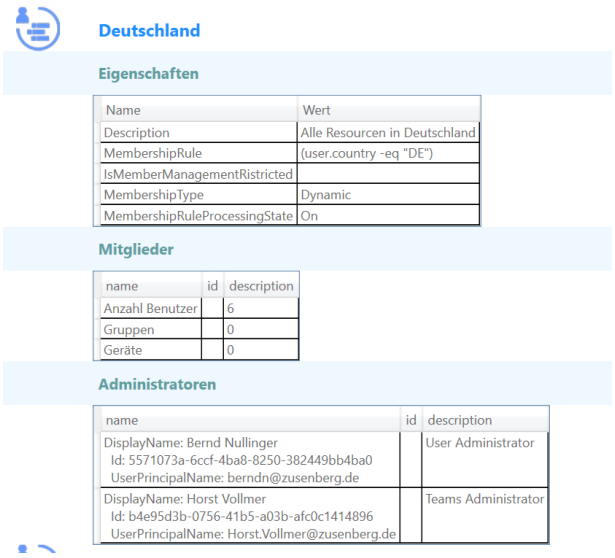
### AAD Apps

Sämtliche registrierten Apps mit:
Name
Beschreibung
Besitzer
Berechtigungen
Hinweis: Anwendungsberechtigungen auf die Microsoft Graph API werden besonders hervorgehoben (unter dem Schraubenschlüssel-Symbol für die App taucht ein Ausrufungszeichen auf.
Bei den Berechtigungen ist jeweils angegeben, ob es sich um delegierte oder Anwendungsberechtigungen handelt.

### AAD Verwaltungseinheiten

Mit Verwaltungseinheiten im Azure Active Directory können Administratorrollen für einzelne Bereiche (Benutzer, Gruppen, Geräte) festgelegt werden.
Eine Beschreibung finden Sie unter https://learn.microsoft.com/de-de/azure/active-directory/roles/administrative-units

Beispiel:




Bei dynamischen Mitgliedschaftsregeln kann enthält das Attribut „MembershipRule“ die Regel für das Erstellen. Im Beispiel enthält die Verwaltungseinheit „Deutschland“ alle Benutzer, bei denen das Länderattribut auf „DE“ gesetzt ist.
Werden Benutzer, Gruppen und Geräte manuell zugeordnet, so sind alle Attribute außer der Beschreibung leer.

Der Tabelle „Mitglieder“ kann die Gesamtzahl der zugeordneten Benutzer, Gruppen und Geräte entnommen werden.

Die Tabelle „Administratoren“ listet die Administratoren und Rollen auf, die dieser Verwaltungseinheit zugeordnet sind. Die Namen der Administratoren werden nur angezeigt, wenn

Sie in den Einstellungen nicht „nur Anzahl der Administratoren anzeigen“ gewählt haben.
In Zukunft sollen auch Richtlinien zum Verhindern von Datenverlust an Verwaltungseinheiten geknüpft werden können. Diese Funktionalität ist derzeit in der Vorschau.

## Privileged Identity Management

Wenn im Tenant E5 Lizenzen vorhanden sind, kann für eine Vielzahl von Rollen das „Privileged Identity Management (PIM)“ genutzt werden. Damit kann erreicht werden, dass Administratoren keine stehenden Berechtigungen haben, sondern Berechtigungen nur dann erteilt werden, wenn sie konkret benötigt werden. Administratoren werden also nicht mehr direkt einer AzureAD Rolle zugewiesen, sondern über PIM verwaltet.  Für die Zuweisungen zu einer Rolle bestehen zwei Möglichkeiten: „active“ oder „eligible“.
Ist eine Zuweisung „active“ braucht sie nicht extra beantragt werden. Es entspricht also quasi der direkten Zuweisung zu einer Rolle. Allerdings kann über PIM das Start- und Endedatum der Zuweisung festgelegt werden, sodass die Berechtigungen nur für einen gewissen Zeitraum verfügbar sind.
Ist eine Zuweisung „eligible“, so muss der Administrator über eine Webseite die Berechtigung beantragen. Die Genehmigung kann automatisch erfolgen oder von festgelegten Personen erteilt werden.

Wenn das „AzureADPreview“ PowerShell Modul installiert ist, kann der Microsoft 365 Checker die PIM Rollen und Zuweisungen auslesen.

Alle verfügbaren Rollen werden dann aufgelistet.
Beispiel:

**Teams Devices Administrator**

Sind für eine Rolle Zuweisungen vorhanden, so werden diese unterhalb der Rolle angezeigt.
Im folgenden Beispiel war der Checker auf „nur Anzahl der Administratoren anzeigen“ eingestellt, daher werden die Namen der berechtigten Admins hier nicht angezeigt.

**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 | |

## Lizenzen

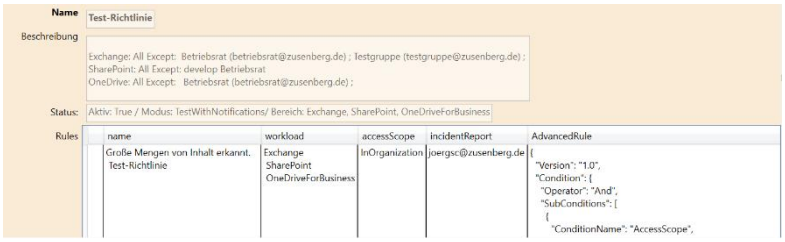
Alle verfügbaren Lizenzen mit:
Anzahl der verfügbaren Lizenzen
Anzahl der zugewiesenen Lizenzen

# Microsoft 365 Security & Compliance

## Data Loss Prevention DLP (Verhindern von Datenverlust)

Alle DLP-Regeln mit:
Name
Beschreibung
Status
Modus
Betroffene Bereiche (Exchange, SharePoint, OneDrive for Business, Teams)
Ausschlüsse aus betroffenen Bereichen
Erweiterte Regeln („Advanced Rules“) – die konkreten Einstellungen der Regeln

Beispiel:




Diese DLP-Regle betrifft die Bereiche (Workloads) Exchange, SharePoint und OneDrive.
Für Exchange sind alle Benutzer ausgeschlossen, die den Gruppen „betriebsrat@zusenberg.de“, oder „testgruppe@zusenberg.de“ angehören.
Aus SharePoint sind die Sites „develop“ und „Betriebsrat“ ausgeschlossen, und für OneDrive alle Mitglieder der Gruppe „betriebsrat@zusenberg.de“.

Da die Anzeige der „AdvancedRules“ she viel Platz benötigen und damit einen Bericht erheblich verlängern können, werden die „AdvancedRules“ in der gefilterten Ansicht nicht dargestellt.

## Aktivitätsbenachrichtigungen

Alle Aktivitätsbenachrichtigungen mit:
Name
Beschreibung
Operation
Nachricht an

## Sicherheitsbenachrichtigungen

Alle Sicherheitsbenachrichtigungen mit:
Name
Beschreibung
Operation
Nachricht an

## AuditLog Aufbewahrungsrichtlinien

Alle Aufbewahrungsrichtlinien mit:
Name
Beschreibung

Status
Operationen
Datentypen
UserIds

### Aufbewahrungsrichtlinien

Alle Aufbewahrungsrichtlinien mit:
Name
Beschreibung
Status
Modus
Workload
Erstellungsdatum
Ersteller
Alle Regeln mit Namen, Abfrage, Typ, Aufbewahrungstagen und Aktion

### Kommunikations-Konformität

Alle Richtlinien zur Kommunikations-Konformität mit:
Name
Beschreibung
Modus
Status
Alle definierten Regeln im JSON Format

### Insider Risiko Management

Alle Richtlinien mit:
Name
Beschreibung
Status
Typ
Szenario
Workload
Ersteller
Letztes Änderungsdatum
Exchange ObjektID

### Inhaltssuche

Alle Inhaltssuchen mit:
Name
Beschreibung
Suche nach
Erstellt von
Letzte Änderung
Ein- und ausgeschlossene Bereiche

### eDiscovery

Hinweis: Um die eDiscoveries auszulesen genügt die Rolle „Globaler Leser“ nicht!

Name
Beschreibung
Status

Letzte Änderung von
Case-Admin

### Advanced eDiscovery

Hinweis: Um die Advanced eDiscoveries auszulesen genügt die Rolle „Globaler Leser“ nicht!

Name
Beschreibung
Status
Letzte Änderung von
Case-Admin

### Data Subject Requests

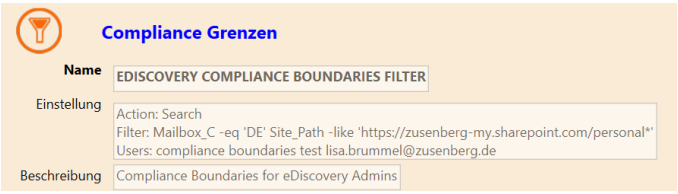
Hinweis: Um die Data Subject Requests auszulesen genügt die Rolle „Globaler Leser“ nicht!

Name
Beschreibung
Status
Erstellt am
Letzte Änderung von
Bearbeiter

### Compliance Grenzen

Alle eingerichteten Compliance-Grenzen mit den dazugehörigen Suchfiltern und Benutzern / Gruppen

Beispiel:



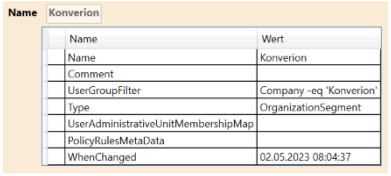

Die Compliance Grenze gilt für alle Benutzer aus der Gruppe „compliance boundaries test“, sowie für „lisa.brummel@zusenberg.de“.

Die Benutzer können – auch wenn ihnen Compliance-Rollen im Compliance Center zugewiesen worden sind- nicht die Postfächer von Benutzern durchsuchen, bei denen das Länderkennzeichen „DE“ eingetragen ist (Filter: Mailbox_C –eq ‚DE‘ / Anmerkung: in Exchange hat das Länderattribut das Kürzel `C`, nicht `country`wie im AzureAD!) und sie können gar keine OneDrive Ordner durchsuchen (Filter: Site_Path -like `https:/zusenberg-my.sharepoint.com/personal*`).

### Informations-Barrieren

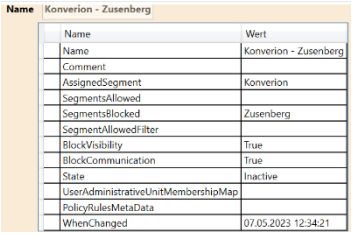
Über „Informations-Barrieren kann die Kommunikation zwischen definierten Benutzergruppen unterbunden werden /betrifft nur Chat und Freigaben, E-Mails können so nicht verhindert werden).

Dazu definiert man zuerst die entsprechenden Segmente, und anschließend die Richtlinien, welche Segmente von welchen isoliert werden sollen.
Beispiel Segmente:




Dem Segment „Konverion“ sind alle Benutzer zugeordnet, bei denen der Firmenname „Konverion“ eingetragen ist.

Beispiel Richtlinie:



Name Konverion - Zusenberg

| | Name | Wert |
|---|---|---|
| | Name | Konverion - Zusenberg |
| | Comment | |
| | AssignedSegment | Konverion |
| | SegmentsAllowed | |
| | SegmentsBlocked | Zusenberg |
| | SegmentAllowedFilter | |
| | BlockVisibility | True |
| | BlockCommunication | True |
| | State | Inactive |
| | UserAdministrativeUnitMembershipMap | |
| | PolicyRulesMetaData | |
| | WhenChanged | 07.05.2023 12:34:21 |

Die Richtlinie ist dem Segment „Konverion“ zugeordnet und verhindert, dass Mitglieder des Segments „Konverion“ solche aus dem Segment „Zusenberg“ sehen, und mit ihnen Chatten oder für sie Dateien freigeben.
Die Beispiel-Richtlinie ist allerdings nicht aktiviert (State: Inactive).

### Rollen

Alle Microsoft 365 Rollen mit:
Name
Beschreibung
Mitglieder (Displaynamen, Name, Vorname, Email Adresse)

## Exchange

### Info

Name der Organisation
Standard-Region
SharePoint URL
Read Tracking
LockBox
Auditing

### Transportregeln

Alle Transportregeln mit:
Name
Beschreibung
Status
Letzte Änderung

### Data Loss Prevention

Alle DLP Regeln mit:
Name
Beschreibung
Status
Modus

### Journal

Alle Journal-Regeln mit:
Name
Überwachte Mailbox / Verteiler
Journal Empfänger
Scope
Modus
Letzte Änderung

### eDiscovery

Alle Exchange eDiscoveries mit:
Name
Beschreibung
Quelle

Zuletzt ausgeführt von
Letzte Ausführung

## Aufbewahrungsrichtlinien

Alle definierten Aufbewahrungsrichtlinien mit:
Name
Beschreibung
Typ
Workload
Erstellungsdatum
Ersteller
Name der dazugehörigen Regeln
Aufbewahrungsdauer
Aufbewahrungstyp
Abfrage
Startzeitpunkt

## Teams

### Nachrichtenrichtlinien

Alle Nachrichtenrichtlinien mit: Name, Beschreibung und den folgenden Parametern:

| Parameter | Bedeutung |
|---|---|
| AllowUrlPreviews | Vorschau von Webseiten anzeigen, wenn eine URL in einen Chat eingefügt wurde<br>Mögliche Werte: true / false |
| AllowOwnerDeleteMessage | Besitzer eines Teams können alle Nachrichten im Team löschen<br>Mögliche Werte: true / false |
| AllowUserEditMessage | Benutzer können eigene Nachrichten ändern<br>Mögliche Werte: true / false |
| AllowUserDeleteMessage | Benutzer können eigene Nachrichten löschen<br>Mögliche Werte: true / false |
| AllowUserChat | Festlegung, ob Benutzer Chats und Kanalnachrichten verfassen können.<br>Mögliche Werte: true / false |
| AllowRemoveUser | Benutzer können andere Benutzer aus Chats entfernen<br>Mögliche Werte: true / false |
| AllowUserTranslation | Benutzer können Nachrichten automatisch übersetzen lassen<br>Mögliche Werte: true / false |
| ReadReceiptsEnabledType | Einstellungen zu Lesebestätigung für Nachrichten<br>Mögliche Werte:<br>UserPreference<br>Jeder Benutzer kann die Einstellung zu Lesebestätigung selbst wählen<br>Everyone<br>Lesebestätigung für alle an<br>None<br>Lesebestätigung für alle aus |
| AudioMessageEnabledType | Legt fest, ob Benutzer Sprachnachrichten senden können.<br>Mögliche Werte<br>ChatsAndChannels<br>Sprachnachrichten können in Chats und Kanalnachrichten erstellt werden<br>ChatsOnly<br>Sprachnachrichten können nur in Chats erstellt werden<br>Disabled<br>Es können keine Sprachnachrichten erstellt werden |
| AllowUserDeleteChat | Benutzer können Chatverläufe aus ihrer Ansicht löschen<br>Mögliche Werte: true / false |
| AllowGiphys | Giphys können in Nachrichten eingefügt werden |

| | |
|---|---|
| | Mögliche Werte: true / false |
| AllowMemes | Memes können in Nachrichten eingefügt werden<br>Mögliche Werte: true / false |
| AllowStickers | Stickers können in Nachrichten eingefügt werden<br>Mögliche Werte: true / false |
| AllowFluidCollaborate | Microsoft Fluid Komponenten können in Nachrichten integriert werden<br>Mögliche Werte: true / false |
| AllowPriorityMessages | Prioritätsnachrichten erlauben<br>Mögliche Werte: true / false |
| AllowSmartReply | In Chats werden Antwortvorschläge angezeigt<br>Mögliche Werte: true / false |
| AllowSmartCompose | Es werden Textvorschläge für Chatnachrichten angezeigt<br>Mögliche Werte: true / false |
| ChannelsInChatListEnabledType | Auf mobilen Geräten werden bevorzugte Kanäle über allen anderen angezeigt<br>DisabledUserOverride<br>Ausgeschaltet, kann vom Benutzer geändert werden<br>EnabledUserOverride<br>Eingeschaltet, kann vom Benutzer geändert werden |
| ChatPermissionRole | Bestimmt die Rolle des Benutzers bei beaufsichtigten Chats.<br>Mögliche Werte:<br>Full<br>der Benutzer kann Chats beaufsichtigen. Aufsichtspersonen haben die Möglichkeit, Chats mit jedem Benutzer innerhalb der Umgebung zu initiieren und einzuladen.<br>Limited<br>Benutzer können Unterhaltungen mit Benutzern mit voller und eingeschränkter Berechtigung initiieren, aber nicht mit begrenzten Benutzern.<br>Restricted<br>Benutzer können nur mit Benutzern mit voller Berechtigung chatten |
| AllowFullChatPermissionUserToDeleteAnyMessage | Benutzer mit der ChatPermissionRole „Full“ können alle Nachrichten löschen<br>Mögliche Werte: true / false |
| AllowVideoMessages | Videonachrichten können erstellt und gesendet werden<br>Mögliche Werte: true/ false |
| AllowCommunicationComplianceEndUserReporting | Benutzer können unangemessene Nachrichten in Chat melden. Nur Verfügbar |

| | |
|---|---|
| | in Verbindung mit E 5 Lizenzen und „Communication Compliance“<br>Mögliche Werte: true / false |

Die Nachrichten-Richtlinie „Global“ ist die Standard-Richtlinie für alle Benutzer.
Wenn nicht alle aufgelisteten Parameter in Ihrem Bericht auftauchen, aktualisieren Sie das PowerShell Modul „MicrosoftTeams“ über den Bereich “Einstellungen / PS“ auf die aktuellste Version.

### Besprechungsrichtlinien

Alle Besprechungsrichtlinien mit: Name, Beschreibung und den folgenden Parametern:

| Parameter | Bedeutung |
|---|---|
| AllowChannelMeetingScheduling | Es können Kanalbesprechungen geplant werden<br>Mögliche Werte: true / false |
| AllowMeetNow | Es können ad-hoc Besprechungen durchgeführt werden<br>Mögliche Werte: true / false |
| AllowPrivateMeetNow | Es können private ad-hoc Besprechungen durchgeführt werden<br>Mögliche Werte: true / false |
| MeetingChatEnabledType | Gibt an, ob Benutzer in Besprechungen chatten können.<br>Mögliche Werte:<br>Disabled, Enabled, EnabledExceptAnonymous |
| LiveCaptionsEnabledType | Live Untertitel in Besprechungen ermöglichen<br>Mögliche Werte:<br>Disabled / DisabledUserOverride |
| AllowIPVideo | Benutzer können in Besprechungen Video benutzen.<br>Mögliche Werte: true / false |
| AllowAnonymousUsersToDialOut | Anonyme Benutzer können Festnetz-Anrufe tätigen.<br>Mögliche Werte: true / false |
| AllowAnonymousUsersToStartMeeting | Anonyme Benutzer können Besprechungen starten.<br>Mögliche Werte: true / false |
| AllowPrivateMeetingScheduling | Benutzer können privare Besprechungen planen.<br>Mögliche Werte: true / false |
| AutoAdmittedUsers | Legt fest, wer die Besprechungslobby automatisch umgeht<br>Mögliche Werte:<br>EveryoneInCompany, EveryoneInSameAndFederatedCompany, Everyone, OrganizerOnly, EveryoneInCompanyExcludingGuests, InvitedUsers |
| AllowCloudRecording | Ermöglicht die Aufzeichnung von Besprechungen<br>Mögliche Werte: true / false |
| AllowOutlookAddIn | Legt fest, ob Benutzer Besprechungen über den Outlook Client planen können.<br>Mögliche Werte: true / false |
| AllowPowerPointSharing | Teilen von PowerPoint Präsentationen in Besprechungen erlauben.<br>Mögliche Werte: true / false |

| | |
|---|---|
| AllowParticipantGiveRequestControl | Benutzer können die Kontrolle über die Bildschirmfreigabe in Besprechungen anfordern.<br>Mögliche Werte: true / false |
| AllowExternalParticipantGiveRequestControl | Externe Benutzer können die Kontrolle über die Bildschirmfreigabe in Besprechungen anfordern.<br>Mögliche Werte: true / false |
| AllowSharedNotes | Geteilte Besprechungsnotizen erlauben<br>Mögliche Werte: true / false |
| AllowWhiteboard | Whiteboard in Besprechungen erlauben.<br>Mögliche Werte: true / false |
| AllowTranscription | Transkription von Besprechungen erlauben.<br>Mögliche Werte: true / false |
| AllowEngagementReport | Für Besprechungen werden Anwesenheitslisten erstellt, die der Organisator herunterladen kann<br>Mögliche Werte: Enabled / Disabled |
| ScreenSharingMode | Festlegung, wie Bildschirminhalte oin Besprechungen geteilt werden können.<br>Mögliche Werte: EntireScreen / SingleApplication |
| AllowPSTNUsersToBypassLobby | Benutzer, die sich per Telefon in eine Besprechung einwählen, können den Warteraum umgehen.<br>Mögliche Werte: true / false |
| AllowOrganizersToOverrideLobbySettings | Besprechungsorganisatoren können die Einstellungen für den Warteraum ändern<br>Mögliche Werte: true / false |
| RecordingStorageMode | Speicherort für Besprechungsaufzeichnungen<br>OneDriveForBusiness |
| AllowCloudRecordingForCalls | Ermöglicht die Aufzeichnung von 1:1 Besprechungen<br>Mögliche Werte: true / false |
| VideoFiltersMode | Erlaubte Bildschirmhintergründe<br>Mögliche Werte:<br>NoFilters, BlurOnly, BlurAndDefaultBackgrounds, AllFilters |
| AllowMeetingReactions | Reaktionen in Besprechungen erlauben<br>Mögliche Werte: true / false |
| AllowMeetingRegistration | Webinare zulassen<br>Mögliche Werte: true / false |
| MeetingRecordingExpirationDays | Aufbewahrungsdauer von Aufzeichnungen in Tagen |
| AllowNDIStreaming | Audio und Video von Besprechungen kann per NDI gestreamt werden<br>Mögliche Werte: true / false |
| SpeakerAttributionMode | Sprechernamen in Aufzeichnungen speichern<br>Mögliche Werte:<br>Disabled, EnabledUserOverride |
| AllowBreakoutRooms | Gruppenräume ermöglichen<br>Mögliche Werte: true / false |
| AllowMeetingCoach | Sprechercoach in Besprechungen zulassen.<br>Mögliche Werte: true / false |
| ChannelRecordingDownload | Aufzeichnungen von Kanalbesprechungen können heruntergeladen werden.<br>Mögliche Werte: Allow / Block |

| | |
|---|---|
| AllowTasksFromTranscript | Es können aus der Transkription heraus Aufgaben erstellt werden.<br>Mögliche Werte: Enabled / Disabled |
| InfoShownInReportMode | Legt fest, welche Informationen in Anwesenheitsberichten verfügbar sind.<br>Mögliche Werte:<br>identityOnly<br>Nur die Namen der Teilnehmer werden erfasst<br>FullInformation<br>Die Namen der Teilnehmer, sowie die genauen Zeiten der Teilnahme (Betreten / Verlassen) werden erfasst |
| QnAEngagementMode | Frage und Antworten Tool in Besprechungen zulassen.<br>Mögliche Werte: Enabled / Disabled |
| AllowAvatarsInGallery | Avatare in der Galerieansicht zulassen:<br>Mögliche Werte: true / false |
| AllowWatermarkForScreenSharing | Wasserzeichen in geteilten Bildschirminhalten zulassen (nur Teams Premium)<br>Mögliche Werte: true / false |
| AllowWatermarkForCameraVideo | Wasserzeichen für Benutzer-Video zulassen (nur Teams Premium)<br>Mögliche Werte: true / false |
| IPAudioMode | Modus für IP-Audio<br>Mögliche Werte:<br>EnabledOutgoingIncoming |
| IPVideoMode | Modus für IP-Video<br>Mögliche Werte:<br>EnabledOutgoingIncoming |
| ExplicitRecordingConsent | Für die Aufzeichnung von Besprechungen wird die Zustimmung aller Teilnehmer angefordert<br>Mögliche Werte: Enabled / Disabled |
| AudibleRecordingNotification | Es erfolgt eine hörbare Ansage, wenn eine Besprechung aufgezeichnet wird<br>Mögliche Werte:<br>PstnOnly |
| CopyRestriction | Legt fest, ob Benutzer in einer Besprechung Chat Nachrichten über die Zwischenablage kopieren können.<br>Mögliche Werte: true / false |
| RoomPeopleNameUserOverride | Es liegt noch keine Beschreibung für diesen Parameter vor.<br>Mögliche Werte: true / false |
| CopilotWithoutTranscript | Dieser Parameter wird nicht mehr genutzt |
| Copilot | Legt fest, ob Copilot mit einem persistenten oder nicht-persistenten Transkript arbeitet.<br>Mögliche Werte:<br>EnabledWithTranscript |
| AutomaticallyStartCopilot | Copilot in Teams wird automatisch gestartet<br>Mögliche Werte; enabled / disabled |

| | |
|---|---|
| VoiceIsolation | Gibt an, ob Benutzer die KI-unterstützte Geräuschunterdrückung in Besprechungen nutzen können.<br>Mögliche Werte: enabled / disabled |
| EnrollUserOverride | Legt fest, ob Benutzer ihre Stimmprofile im Teams Client registrieren können.<br>Mögliche Werte: enabled / disabled (Standard) |
| RoomAttributeUserOverride | Legt fest, ob Benutzer in Teams-Räumen aufgrund ihrer Stimme erkannt werden können.<br>Mögliche Werte:<br>**Off**<br>Teams-Room Benutzer werden nicht erkannt. Die Stimmprofile der Benutzer werden nicht genutzt.<br>**Attribute**<br>Wenn Benutzer ihr Stimmprofil registriert haben, wird dieses genutzt um die Benutzer zu identifizieren und mit Namen zu versehen.<br>**Distinguish**<br>Wenn Benutzer ihr Stimmprofil registriert haben, wird dieses genutzt um die Benutzer zu identifizieren, aber die Benutzer werden nur mit „Sprecher (n)“ markiert. |

## Webinar Richtlinien

| Parameter | Bedeutung |
|---|---|
| AllowWebinars | Benutzer können Webinare erstellen<br>Mögliche Werte:<br>Enabled / Disabled |
| Description | Beschreibung der Richtlinie |
| EventAccessType | Legt fest, wer sich für Webinare registrieren kann.<br>Mögliche Werte:<br>Everyone – jeder kann sich registrieren, einschließlich Gäste und Externe<br>EveryoneInCompanyExcludingGuest: es können sich nur Benutzer der eigenen Tenants registrieren |
| AllowTownHalls | Derzeit noch keine Auswirkung<br>Mögliche Werte:<br>Enabled / Disabled |
| AllowEmailEditing | Derzeit noch keine Auswirkung<br>Mögliche Werte:<br>Enabled / Disabled |

## Liveereignis-Richtlinien

Alle Liveereignis-Richtlinien mit Name, Beschreibung und folgenden Parametern:

| Parameter | Bedeutung |
|---|---|
| AllowBroadcastScheduling | Benutzer können Live-Ereignisse planen<br>Mögliche Werte: true / false |
| AllowBroadcastTranscription | Live-Ereignisse können transkribiert werden.<br>Mögliche Werte: true / false |
| BroadcastAttendeeVisibilityMode | Legt fest, wer an Live-Ereignissen teilnehmen kann.<br>Mögliche Werte:<br>Everyone, EveryoneInCompany. InvitedUsersInCompany, EveryoneInCompanyAndExternal, InvitedUsersInCompanyAndExternal |
| BroadcastRecordingMode | Aufzeichnungs-Modus für Live-Ereignisse<br>Mögliche Werte:<br>AlwaysEnabled, AlwaysDisabled, UserOverride |

## KI-Richtlinien

Über die KI-Richtlinien werden die Möglichkeiten der Benutzer, ihr Stimmprofil für die intelligente Geräuschunterdrückung und ihr Gesichtsprofil für die Personenerkennung in Teams-Räumen zu registrieren ein- oder ausgeschaltet.

| Parameter | Bedeutung |
|---|---|
| Identity | Name der Richtlinie |
| EnrollVoice | Benutzer können Stimmprofil registrieren<br>Mögliche Werte: enabled / disabled |
| EnrollFace | Benutzer können Gesichtsprofil registrieren<br>Mögliche Werte: enabled / disabled |

### Arbeitsplatz Erkennung

Über die Einstellung zur Arbeitsplatz-Erkennung wird festgelegt, ob der aktuelle Arbeitsplatz eines Benutzer in Teams-Räumen oder bei buchbaren Schreibtischen automatisch erkannt und im Status veröffentlicht werden kann.
Benutzer müssen dies zusätzlich über Einstellungen in ihrem Teams Client aktivieren (Einstellungen – Datenschutz – Meinen Arbeitsplatz verwalten).

| Parameter | Bedeutung |
|---|---|
| Identity | Name der Richtlinie |
| EnableWorkLocationDetection | Der Arbeitsort eines Benutzers kann automatisch erkannt und veröffentlicht werden.<br>Mögliche Werte: True / False (Standard) |

### App Berechtigungen

Alle App Berechtigungs-Richtlinien mit Namen und folgenden Parametern:

| Parameter | Bedeutung |
|---|---|
| DefaultCatalogApps | Liste der Microsoft Apps |
| GlobalCatalogApps | Liste der Drittanbieter-Apps |
| PrivateCatalogApps | Liste der selbst erstellten Apps |
| DefaultCatalogAppsType | Einstellung, ob die Liste der Microsoft Apps die erlaubten, oder die blockierten Apps enthält<br>Mögliche Werte:<br>BlockedAppList, AllowedAppList |
| GlobalCatalogAppsType | Einstellung, ob die Liste der Drittanbieter- Apps die erlaubten, oder die blockierten Apps enthält<br>Mögliche Werte:<br>BlockedAppList, AllowedAppList |
| PrivateCatalogAppsType | Einstellung, ob die Liste der selbst erstellten Apps die erlaubten, oder die blockierten Apps enthält<br>Mögliche Werte:<br>BlockedAppList, AllowedAppList |

### Richtlinien zur Compliance Aufzeichnungen

Alle Richtlinien zur Compliance Aufzeichnung von Gesprächen mit:
Name
Beschreibung
Status
Registrierte Anwendung

## Microsoft Viva

### Viva Insights

Alle für Viva definierten Rollen, sowie deren Inhaber.

Hinweis: Nur Mitglieder der Rolle „Analyst“ können eigene, über die vordefinierten Analysen von Viva Insights hinausgehenden, Abfragen und Auswertungen erstellen. Mitgliedern dieser Rollengruppe stehen also alle Funktionalitäten des ehemaligen Workplace Analytics zur Verfügung!

## Selbstbedienungseinkäufe

Hier werden alle Produkte angezeigt, für die Microsoft Selbstbedienungseinkäufe ermöglicht:

| | Dienst | 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 |

Die möglichen Werte unter „Settings „ sind:

| **Setting** | **Auswirkung** |
|---|---|
| Enabled | Benutzer können Selbstbedienungseinkäufe tätigen und sich für Testversionen registrieren |
| OnlyTrialsWithoutPaymentMethod | Benutzer können keine Selbstbedienungseinkäufe tätigen, aber sie können kostenlose Testversionen von Produkten erwerben, für die sie keine Zahlungsmethode angeben müssen. Nach Ablauf der Testversion kann ein Nutzer die kostenpflichtige Version des Produkts nicht kaufen. |
| Disabled | Benutzer können **keine** Selbstbedienungseinkäufe tätigen und sich **nicht** für Testversionen registrieren |

## Einstellungen der Organisation

### Generelle Einstellungen

Primärer Name des Tenants
Sprache für Benachrichtigungen
Technischer Kontakt
Datenschutzkontakt
Datenschutz-URL

### Datenspeicherort

Die Datenspeicherorte (data-at-rest location) für
Exchange
SharePoint
Teams
ExchangeOnlineProtection
Viva Topics
Viva Connections
OneDrive for Business

Angabe ob Multi-Geo genutzt wird (true/false)

### Lockbox

Angabe, ob Customer-Lockbox aktiviert ist (true / false)

### Einführungsbewertung

| Parameter | Bedeutung |
|---|---|
| ProductivityScoreOptedIn | Gibt an, ob alle Benutzer und Gruppen für die Berechnung der Produktivitätsbewertung herangezogen werden<br>Mögliche Werte: true / false |
| OperationUserPuid | |
| OperationTime | |

### Graph Data Connect

| Parameter | Bedeutung |
|---|---|
| ServiceEnabled | Dienst aktiviert? Mögliche Werte: true / false |
| TenantLockBoxApproverGroup | Standardgenehmigungsgruppe, die Zugriffe freigeben muss |
| TenantLockBoxDataAccessPolicyType | Richtlinientyp für Zugriffe über Graph Data Connect |
| IsOdspEnabled | Zugriff auf OneDrive und SharePoint erlaubt?<br>Mögliche Werte: true/ false |
| IsCrossTenantDataMovementEnabled | Datenübertragung in anderen Tenant erlaubt?<br>Mögliche Werte: true/ false |
| IsVivaInsightsEnabled | Viva Insights eingeschaltet?<br>Bezieht sich nicht auf Viva Personal Insights, sondern das ehemalige Workplace Analytics<br>Mögliche Werte: true/ false |

### Berichte

Mit „Berichte“ sind die Verwendungsberichte in den verschiedenen Admin-Centern gemeint.

| Parameter | Bedeutung |
|---|---|

| | |
|---|---|
| GraphApiEnabled | Zugriff per Graph-API erlaubt?<br>Mögliche Werte: true/ false |
| PowerBiEnabled | Berichtsdaten für Power BI zur Verfügung stellen?<br>Mögliche Werte: true/ false |
| PrivacyEnabled | Pseudonyme Bezeichner in allen Berichten verwenden?<br>Mögliche Werte: true/ false |
| Region | Region, in der die Daten verarbeitet werden |
| TenantId | GUID des Tenants |
| PBIStatusUpdateDate | Datum und Uhrzeit, wann die Verwendungsdaten zuletzt an Power BI übertragen wurden |
| PBIStatus | PowerBI Verarbeitungs-Status<br>Möglicher Werte: completed |

## Bookings

| Parameter | Bedeutung |
|---|---|
| Enabled | Bookings für den gesamten Tenant ein-/ausschalten<br>Mögliche Werte: true/ false |
| SocialSharingRestricted | Der „Mit Facebook verbinden“ Schalter wird entfernt |
| BookingsExposureOfStaffDetailsRestricted | Es werden keine Mitarbeiterdaten in der Kommunikation mit Kunden versendet<br>Mögliche Werte: true/ false |
| StaffMembershipApprovalRequired | Benutzer müssen die Freigabe ihres Kalenders in Bookings beantragen und als Mitarbeiter in Bookings eingetragen werden<br>Mögliche Werte: true/ false |
| BookingsSmsMicrosoftEnabled | Microsoft kann SMSe zur Terminbestätigung an Kunden versenden<br>Mögliche Werte: true/ false |
| BookingsSearchEngineIndexEnabled | Verhindert, dass die Buchungsseiten von Bookings in Suchergebnissen von Bing oder Google auftauchen<br>Mögliche Werte: true/ false |
| BookingsNamingPolicyEnabled | Namenskonventionen für die Bookings-Kalender durchsetzen<br>Mögliche Werte: true/ false |
| Weitere Parameter | Erläuterungen zu den weiteren Parametrn finden Sie unter https://learn.microsoft.com/de-de/microsoft-365/bookings/turn-bookings-on-or-off?view=o365-worldwide |

## Forms

| Parameter | Bedeutung |
|---|---|
| ExternalCollaborationEnabled | Zusammenarbeit mit Externen ermöglichen<br>Mögliche Werte: true/fasle |
| ExternalSendFormEnabled | Externen kann ein Link zum Formular gesendet werden, um Antworten zu sammeln<br>Mögliche Werte: true/fasle |
| ExternalShareCollaborationEnabled | Formular kann gemeinsam mit Externen bearbeitet werden<br>Mögliche Werte: true/false |
| ExternalShareTemplateEnabled | Formular kann els Vorlage mit Externen geteilt werden |

| | |
|---|---|
| | Mögliche Werte: true/false |
| ExternalShareResultEnabled | Ergebnisszusammenfasuung eines Formulars kann mit Externen geteilt werden<br>Mögliche Werte: true/false |
| RecordIdentityByDefaultEnabled | Namen standardmäßig erfassen<br>Mögliche Werte: true/false |
| BingImageSearchEnabled | Das Hinzufügen von Bildern von Bing und aus YouTube-Videos in Forms gestatten |
| InOrgFormsPhishingScanEnabled | Internen Schutz vor Pishing aktivieren<br>Mögliche Werte: true/false |
| InOrgSurveyIncentiveEnabled | Derzeit nicht genutzt |

## Cortana

| Parameter | Bedeutung |
|---|---|
| Enabled | Erlauben Sie Cortana unter Windows 10 und der Cortana App unter iOS und Android auf die von Microsoft gehosteten Daten im Auftrag von Personen in Ihrer Organisation zuzugreifen.<br>Cortana verwendet diese Daten, um Mitarbeitern in Ihrer Organisation zu helfen, auf dem Laufenden zu bleiben und Erkenntnisse über ihre Besprechungen, Dokumente und Beziehungen zu erhalten.<br>Mögliche Werte: true/false |

## MyAnalytics

Diese Einstellungen gelten für alle Benutzer.

| Parameter | Bedeutung |
|---|---|
| EnableInsightsDashboard | Das Viva Dashboard erlauben (Viva Insights (office.com))<br>Mögliche Werte: true/false |
| EnableWeeklyDigest | Wöchentliche E-Mail Zusammenfassung an Benutzer senden (Kann vom Benutzer überschrieben werden)<br>Mögliche Werte: true/false |
| EnableInsightsOutlookAddIn | Das Insights- AddIn in Outlook erlauben<br>Mögliche Werte: true/false |

## Elementeinblicke

| Parameter | Bedeutung |
|---|---|
| AllowItemInsights | Elementeinblicke für alle Benutzer einschalten<br>(Wenn die Elementeinblicke generell erlaubt sind, können sie von jedem Benutzer in seinen Datenschutzeinstellungen abgeschaltet werden)<br>Mögliche Werte: true/false |
| DisabledForGroup | Die Elementeinblicke sind für bestimmte Benutzergruppen abgeschaltet.<br>Mögliche Werte: true/false |
| DisabledForGroupID | Wenn die Elementeinblicke für bestimmte Gruppen abgeschaltet sind, stehen hier die IDs der Gruppen |

### Besprechungseinblicke

| Parameter | Bedeutung |
|---|---|
| AllowMeetingInsights | Besprechungseinblicke sind für alle Benutzer im Tenant eingeschaltet<br>Mögliche Werte: true/false |

### Lizenzen

Inhaltlich die gleichen Informationen wie im Bereich Lizenzen im Azure Active Directory, allerdings werden hier die verständlichen Namen der Lizenzen mit angezeigt.

Also beispielsweise nicht nur STANDARDWOFFPACK_STUDENT sondern auch der dazugehörige Name „Office A1 for students“.