Konverion

Microsoft 365 Checker

Handbuch

Version 8.5

Konverion GmbH
Straße der Jugend 18
14974 Ludwigsfelde
Geschäftsführer: Jörg Schanko

Amtsgericht Potsdam
HRB: 41452 P
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 zur aktuellen Versionen des Checkers 6
Telemetrie 6
Lizensierung 6
Vorbereitung 8
Installation 9
Generelle Vorgehensweise 11
Vorlagen erstellen 12
Eine neue Vorlage erstellen 12
Vorlagen bearbeiten 13
Vorlagen löschen 13
Berichte erstellen 14
Neue Berichte erstellen 14
Berichte ansehen 16
Gefilterte Berichte ansehen 16
Vergleichsgrundlage festlegen 17
Bericht als Word Dokument speichern 17
Bericht löschen 18
Bericht exportieren 18
Bericht importieren 18
Berichte vergleichen 20
Detailvergleich 21
Übersicht des Vergleichs in Word exportieren 22
Einstellungen 23
Allgemein 23
Daten 23
PS (PowerShell) 23
Cert (Zertifikat-basierte Anmeldung einrichten) 24
Schritt 1 Anwendung in Entra ID registrieren 24
Berechtigungstypen 27
Schritt 2 – Zertifikat erstellen 27
Schritt 3 – Zertifikat in der registrierten App importieren 28
Schritt 4 - Erteilen der notwendigen Berechtigungen 28
Schritt 5 – Anmeldedatei erstellen 28
Lizenz 31

Übersicht 31
Problembehandlung 32
Der Microsoft 365 Checker lässt sich nicht installieren 32
Installation der PowerShell Module 32
Anhang: Auslesbare Einstellungen 34
Unified Audit Log 34
Azure Active Directory 35
Info 35
AAD Rollen 35
AAD Apps 35
AAD Verwaltungseinheiten 35
Privileged Identity Management 36
Lizenzen 37
Microsoft 365 Security & Compliance 37
Data Loss Prevention DLP (Verhindern von Datenverlust) 37
Aktivitätsbenachrichtigungen 37
Sicherheitsbenachrichtigungen 37
AuditLog Aufbewahrungsrichtlinien 37
Aufbewahrungsrichtlinien 38
Kommunikations-Konformität 38
Insider Risiko Management 38
Inhaltssuche 38
eDiscovery 38
Advanced eDiscovery 39
Data Subject Requests 39
Compliance Grenzen 39
Informations-Barrieren 39
Rollen 40
Exchange 40
Info 40
Transportregeln 40
Data Loss Prevention 40
Journal 40
eDiscovery 40
Aufbewahrungsrichtlinien 41
Teams 42

Nachrichtenrichtlinien 42
Besprechungsrichtlinien 44
Webinar Richtlinien 48
Liveereignis-Richtlinien 48
KI-Richtlinien 48
Arbeitsplatz Erkennung 49
App Berechtigungen 49
Richtlinien zur Compliance Aufzeichnungen 49
Microsoft Viva 49
Viva Insights 49
Selbstbedienungseinkäufe 50
Einstellungen der Organisation 51
Generelle Einstellungen 51
Datenspeicherort 51
Lockbox 51
Einführungsbewertung 51
Graph Data Connect 51
Berichte 51
Bookings 52
Forms 52
Cortana 53
MyAnalytics 53
Elementeinblicke 53
Besprechungseinblicke 54
Integrated Apps Settings 54
Viva Modules 54
Lizenzen 54
Copilot 55
Lizenzen 55
Copilot Selbstbedienungseinkäufe 55
Flex Routing 55
Teams 55
Copilot in Víva 56
Admin Center 56
Video Generierung 57
Bild Generierung 57

3rd Party Modelle 57
Frontier 58
Opal 58

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 zur aktuellen Versionen des Checkers

Ab der Version 8.2 werden für den Checker nur noch die PowerShell Module für Exchange und Teams genutzt. Alle weiteren, früher benötigten, Module wurden durch direkte Verwendung verschiedener Programmierschnittstellen (APIs) ersetzt.

Die Authentifizierung basiert jetzt vollständig auf der „Microsoft Authentication Library (MSAL)“. Für die Anmeldung per Benutzername ist damit die Registrierung einer App in Entra ID nicht mehr erforderlich. Eine in Entra ID registrierte App wird nur noch für die Anmeldung per Zertifikat benötigt.

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

Um den Microsoft 365 Checker sinnvoll einsetzen zu können, benötigt der jeweilige Benutzer ausreichende Berechtigungen in Microsoft 365, um die Konfigurationen auslesen zu können. Ausgenommen hiervon ist die Zertifikat-basierte Anmeldung, für die jedoch einige Vorbereitungen getroffen werden müssen (siehe „Cert (Zertifikat-basierte Anmeldung einrichten)“).

Die Berechtigungen lassen 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 Reader“ 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 Checkers einfacher im Microsoft 365 Ereignisprotokoll nachvollzogen werden.

Im Rahmen dieses Handbuches werden das Konto „braudit@zusenberg.de“ genutzt.

Damit der Microsoft 365 Checker in Ihrem Microsoft 365 Tenant die Teams, Exchange und Compliance Konfigurationen auslesen kann, benötigt er (derzeit noch) einige PowerShell Module.

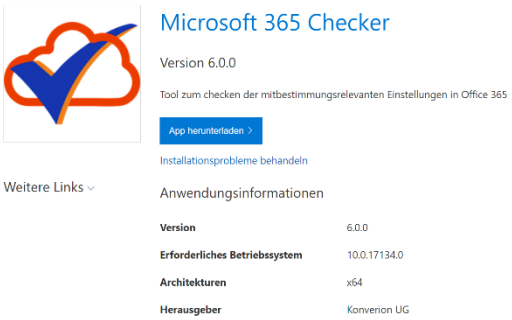
Für die initiale Installation der notwendigen PowerShell Module müssen Sie Administratorrechte auf dem lokalen PC haben. Dies ist aber nur für die Installation der „NuGet“ PowerShell Module notwendig. Diese werden benötigt, um Module in der Microsoft PowerShell Galerie (https://www.powershellgallery.com/) 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

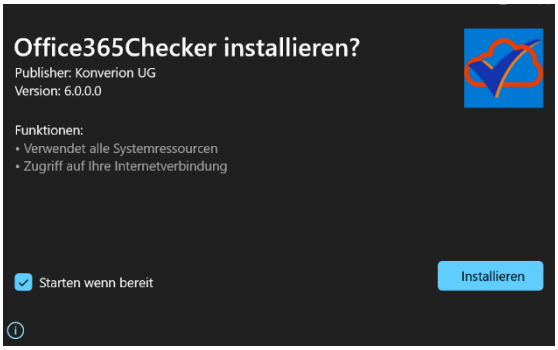
Der Microsoft 365 Checker wird durch sogenanntes „querladen“ installiert. Dieses muss auf Ihrem PC erlaubt sein (Hinweis: Die Installation des Checkers auf einem Server-Betriebssystem, einschließlich Terminalserver-Session, wird nicht unterstützt). Stellen Sie unter „Einstellungen“ – „Update und Sicherheit“ – „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“.

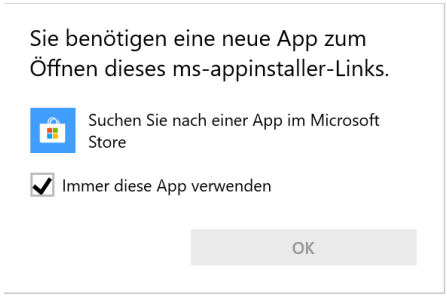


Es erscheint ein Dialogfenster, in dem Sie auf „Installieren“ klicken.

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:

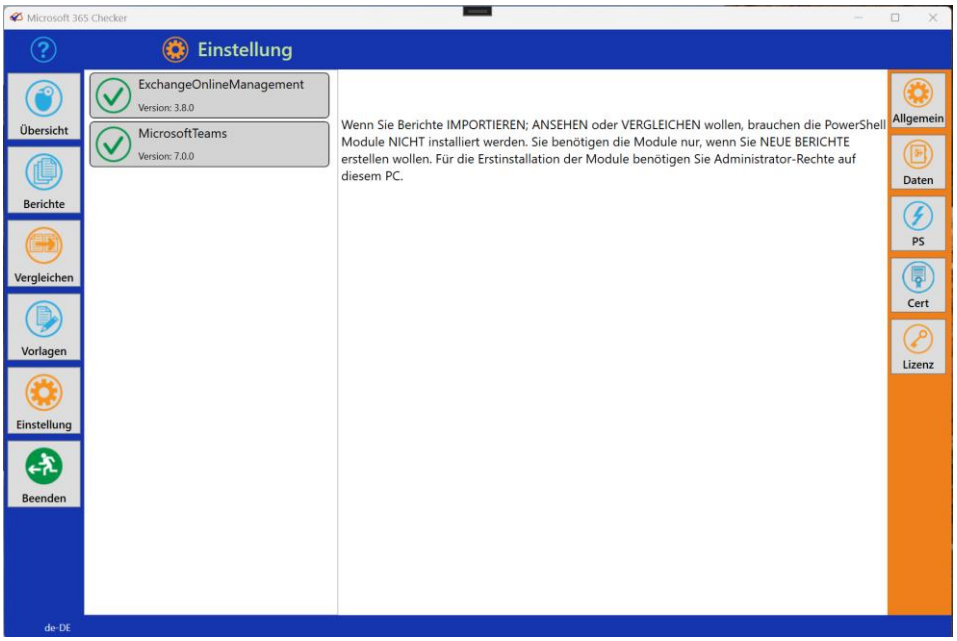
Starten Sie in diesem Fall die Windows PowerShell ISE als Administrator, laden Sie das Script c:\data\office365checker\installNuGet.ps1 ünd führen es aus.

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 4 Unterordner enthalten:

- ExchangeOnlineManagement
- MicrosoftTeams
- PackageManagement
- PowerShellGet

Sie sollten nun dieses Ergebnis sehen:



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.

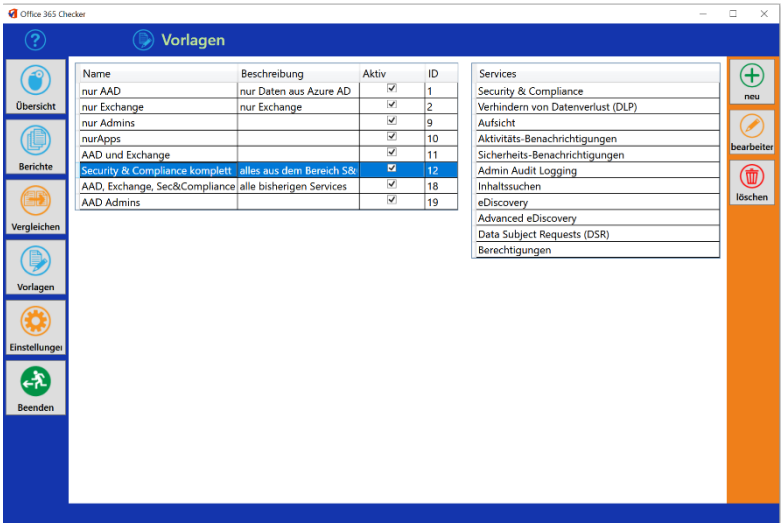
Vorlagen erstellen

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

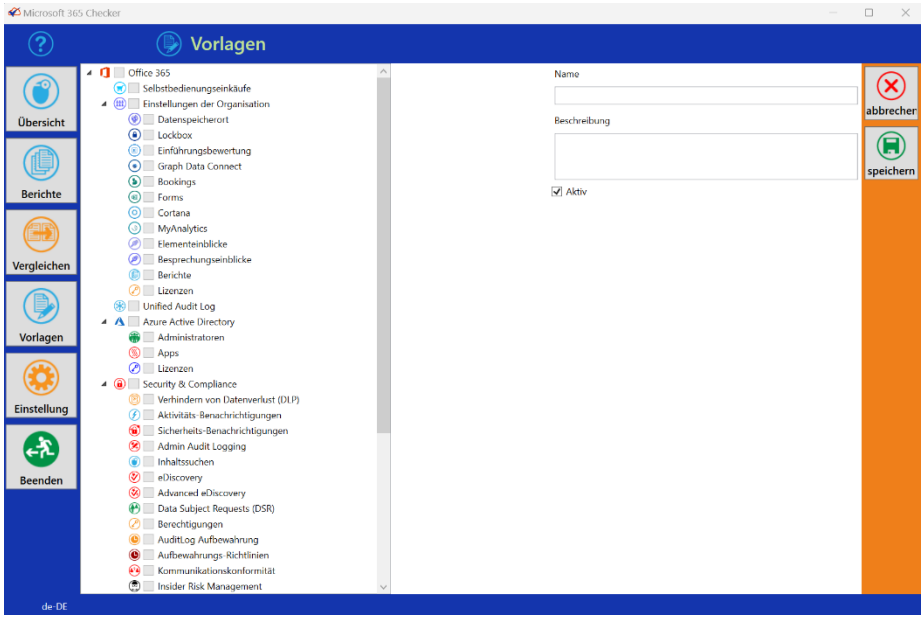
Sie erhalten eine Ansicht der bereits definierten Vorlagen:



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.

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.

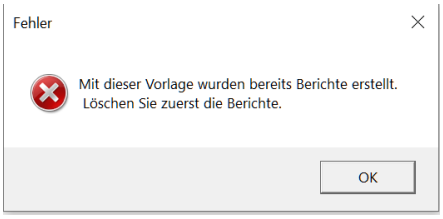
Vorlagen bearbeiten

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

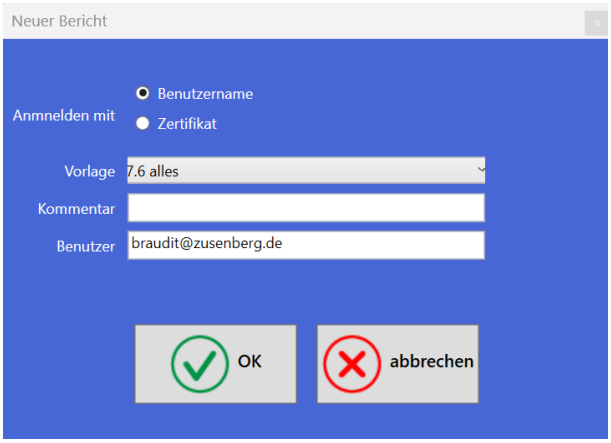
Klicken Sie im Bereich „Berichte“ auf

um einen neuen Bericht zu erstellen.

Hinweis:
Sollte der Schalter „Neu“ ausgegraut und damit nicht verfügbar sein, so ist entweder

- der Demo-Zeitraum abgelaufen,
- die Lizenz abgelaufen, oder
- kein PowerShell Modul installiert

In dem nun erscheinenden Dialogfenster wählen Sie zuerst die Anmeldemethode aus.
Die Option „Zertifikat“ erscheint nur, wenn mindestens ein Zertifikat im Checker eingerichtet ist.
Sehen Sie hierzu „Zertifikat-basierte Anmeldung einrichten“

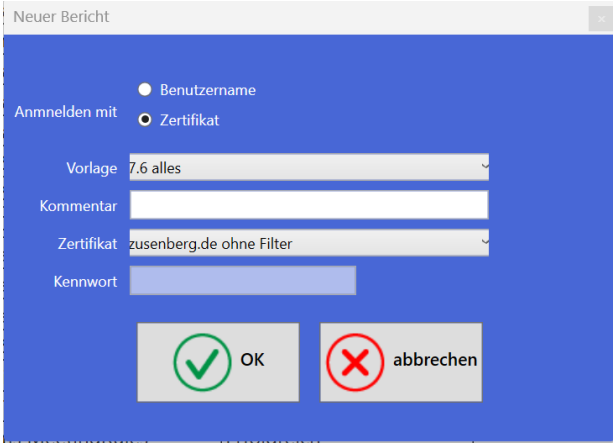


Bei der Anmeldung per Benutzername erfolgt die Abfrage des Kennwortes erfolgt interaktiv, nachdem Sie auf „OK“ geklickt haben.

Bei der ersten Anmeldung erscheint der Dialog

Klicken Sie hier unbedingt auf „Ja“, da der Checker sich zum Erstellen von Berichten mit mehreren Diensten verbinden muss (Entra, Exchange, Teams,…).

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“.

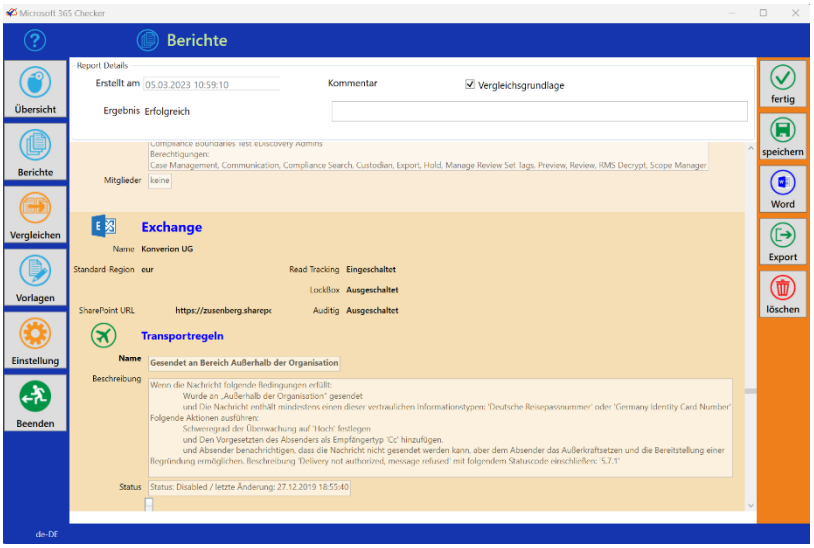
Je nach Menge der zu lesenden Konfigurationen kann die Erstellung eines Berichtes mehrere Minuten bis zu einigen Stunden in Anspruch nehmen.

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

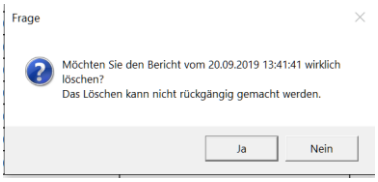
Um einen Bericht als Word Dokument zu speichern, muss Microsoft Word auf dem PC installiert sein. Wählen Sie im Bereich „Berichte“ den gewünschten Bericht aus und klicken Sie anschließend auf „ansehen“. Daraufhin wird Ihnen der gewählte Bericht angezeigt. Klicken Sie auf den Schalter „Word“. Es wird 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.

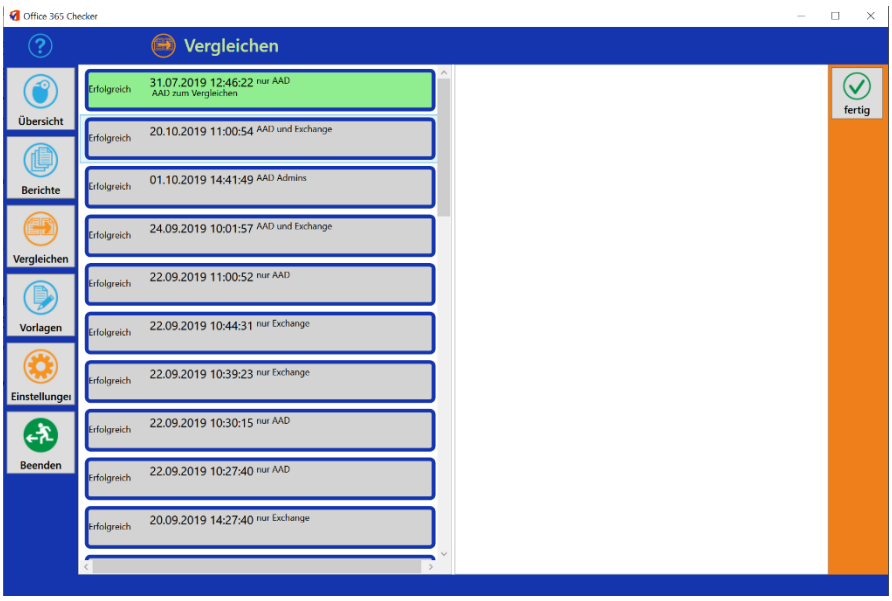
Hinweis:

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.

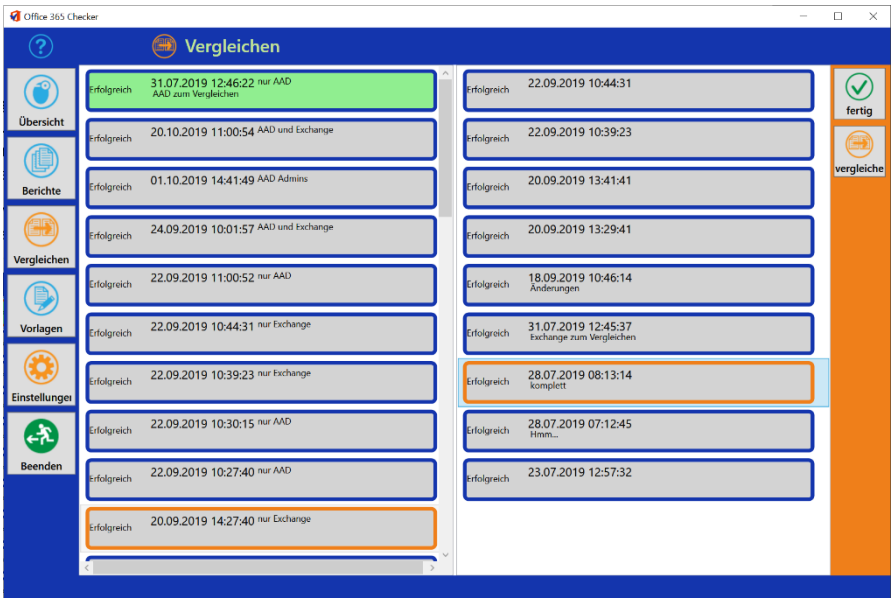
Um Berichte miteinander zu vergleichen wählen Sie den Bereich „Vergleichen“.



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.

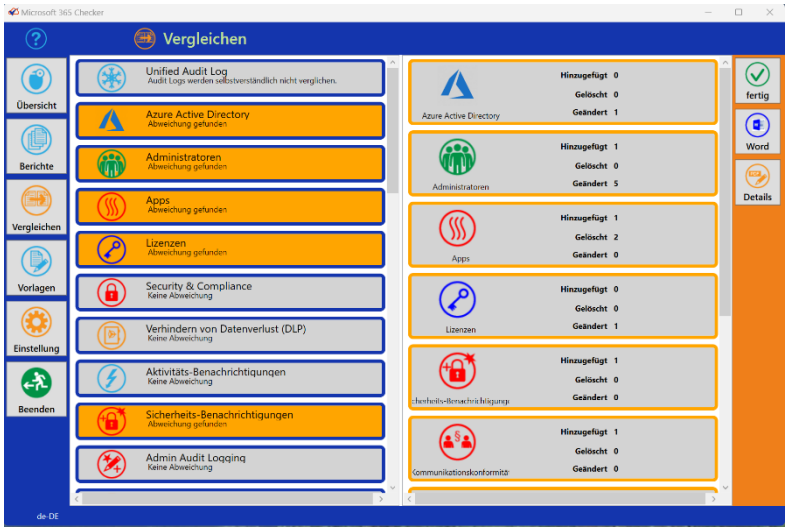


Wählen Sie aus der rechten Liste den Bericht aus, mit dem der orange markierte Bericht der linken Liste verglichen werden soll.

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 mehrere 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

Dies bezieht sich insbesondere auf die Exchange-Funktionalitäten „Beweissicherung“ und „Journal“, da diese explizit für bestimmte Benutzer angewendet werden.

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.

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

Daten

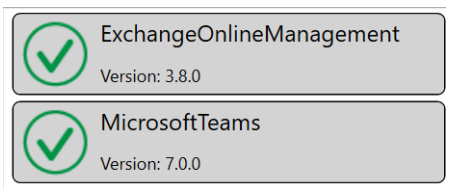
Hier sehen Sie den aktuellen Pfad zur Datenbank (Office365Checker.db3). Bei Bedarf können Sie die Datenbank über den Schalter „verschieben“ auf eine andere Festplatte oder in ein anderes Verzeichnis verschieben. Solange keine gewichtigen Gründe vorliegen, sollten Sie die Datenbank jedoch dort belassen,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

- Exchange Online Management, sowie
- Microsoft Teams

installiert.

Weitere PowerShell sind ab der Version 8.2 des Checkers nicht mehr erforderlich.

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.

Cert (Zertifikat-basierte Anmeldung einrichten)

Diese Art der Authentifizierung ist nur dann erforderlich, wenn Benutzer ohne administrative Berechtigungen (z.B. Betriebsräte) die Möglichkeit bekommen sollen, Berichte selbst zu erstellen. Bei der Anmeldung per Zertifikat bestehen derzeit technisch bedingt folgende Einschränkungen:

- Die „Einstellungen der Organisation“ können nicht ausgelesen werden
- Die Audit Logs könne nicht ausgelesen und ausgewertet werden
- Die Einstellungen zu Copilot können nicht ausgelesen werden

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

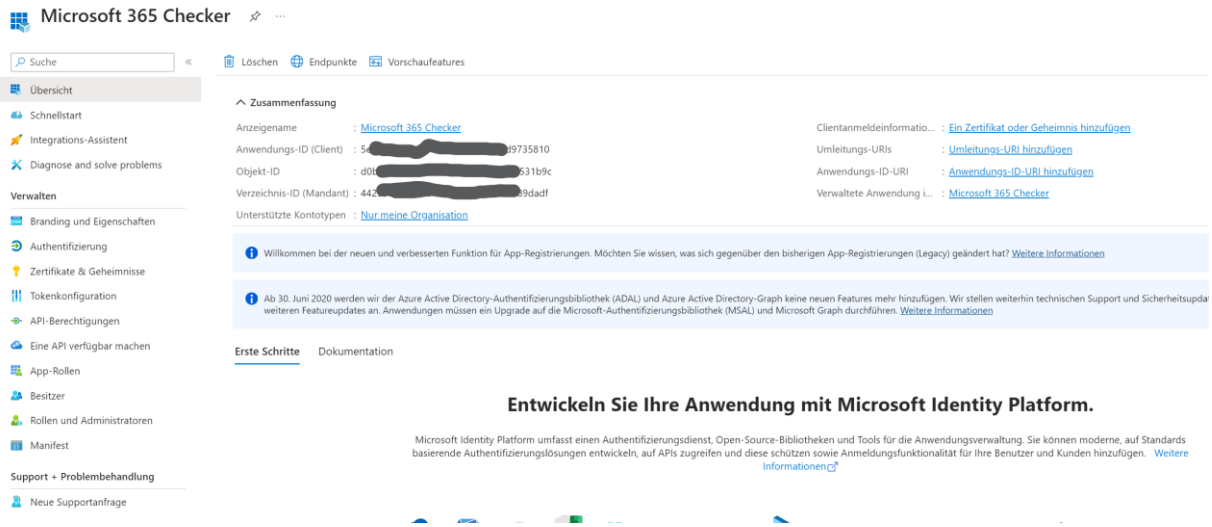
1) Registrieren einer Anwendung in Entra ID
2) Erstellen eines selbst-signierten Zertifikates, bzw. Export der entsprechenden Zertifikats-Dateien aus Ihrer eigenen PKI
3) Registrieren des Zertifikats in der Entra ID App
4) Erteilen der notwendigen Berechtigungen
5) Erstellen einer Anmeldedatei

Schritt 1 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 Microsoft-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 „AppCatalog“ und markieren „AppCatalog.Read.All“.

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“.

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“.
Klicken Sie auf „Anwendungsberechtigungen“ und aktivieren „Policy.Read.AllowSelfServicePurchase“.

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

Bestätigen Sie mit „Berechtigungen hinzufügen“.

Hinweis: Der „LicenseManager“ dient zum Auslesen der Einstellungen zu den Selbstbedienungs-Einkäufen.

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 (1)				
Policy.Read.AllowSelfServiceP	Anwendung	Read AllowSelfServicePurchase policy settings	Ja	Gewährt für "Konverion ...
Microsoft Graph (6)				
AppCatalog.Read.All	Anwendung	Read all app catalogs	Ja	Gewährt für "Konverion ...
Application.Read.All	Anwendung	Read all applications	Ja	Gewährt für "Konverion ...
Directory.Read.All	Anwendung	Read directory data	Ja	Gewährt für "Konverion ...
RoleManagement.Read.All	Anwendung	Read role management data for all RBAC providers	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 ...

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

Bereich	Berechtigung	Zweck
Microsoft Graph	AppCatalog.Read.All	Freigegebene Apps in Teams auslesen
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.All	Auslesen der administrativen Rollen
M365 License Manager	Policy.Read.AllowSelfServicePurchase	Einstellungen für Selbstbedienungseinkäufe auslesen
Exchange	Exchange.ManageAsApp	Der Anwendung Zugriff auf die Exchange und Purview 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“.

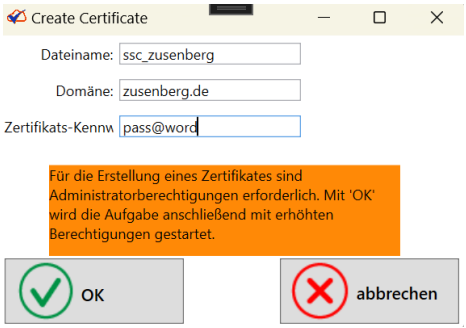
„Delegiert“ bedeutet, die Anwendung, die auf Daten über die Programmierschnittstelle zugreifen möchte, tut dies im Namen des Benutzers, also auch genau mit den Berechtigungen, die dieser Benutzer bereits hat. Über delegierte Berechtigungen werden also keine weiteren Berechtigungen vergeben, sondern lediglich 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.

Schritt 2 – 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.

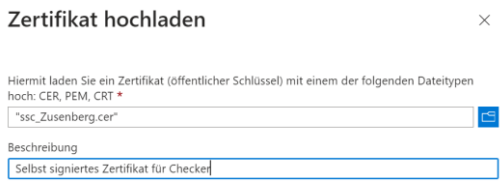
Die Dateien finden Sie im Verzeichnis „C:\data\office365checker\certs“. Bei Verwendung des oben benutzen Dateinamens finden Sie in diesem Verzeichnis nun die Dateien „ssc_Zusenberg.cer“ (Zertifikatdatei) sowie „ssc_Zusenberg.pfx“ (Privater Schlüssel).

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 3 – 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 4 - Erteilen der notwendigen Berechtigungen

Da die Einstellungen für Teams und Exchange (und damit auch für Purview) noch per PowerShell ausgelesen werden, muss die gerade registrierte Anwendung der Administrativen Rolle „Globaler Leser“ hinzugefügt werden, um über ausreichende Berechtigungen zum Auslesen der Konfiguration zu verfügen. Diese Berechtigung wird über den ServicePrincipal der registrierten App erteilt.

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“.

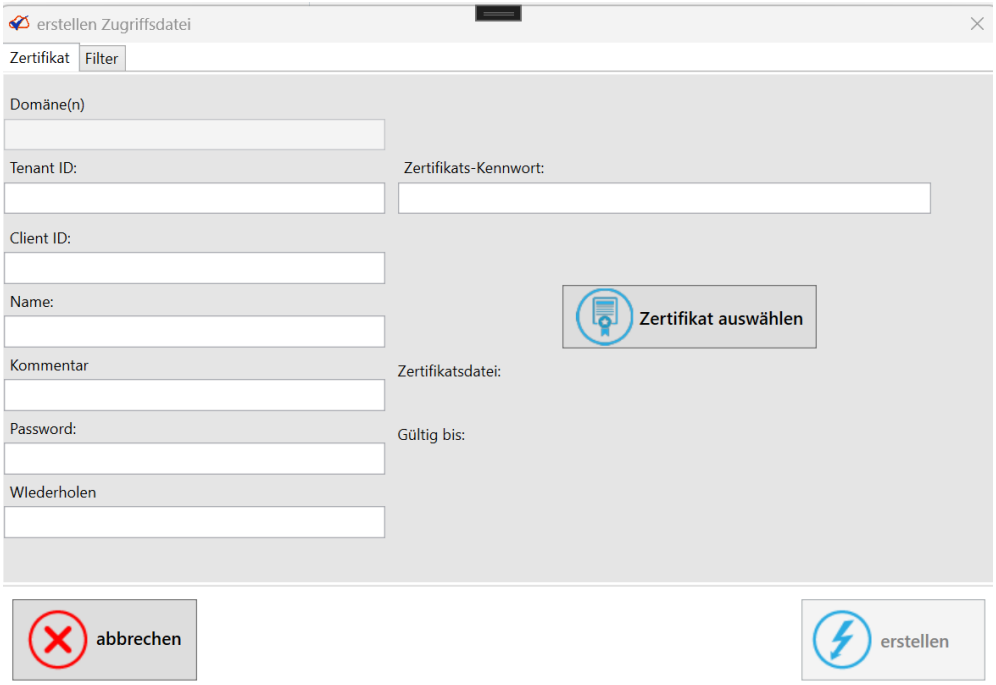
Der ServicePrincipal der App wird jetzt in der Liste der Zuweisungen angezeigt.

Um die Purview-Rollen auslesen zu können, muss die registrierte Anwendung ebenfalls der Rolle „Compliance Administrator“ hinzugefügt werden.

Schritt 5 – Anmeldedatei erstellen

Über die Anmeldedatei wird der Ersatz für den „gekapselten Modus“ aus älteren Checker-Versionen 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 zuerst das Zertifikats- 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.

Tragen Sie die Tenant ID und die Client ID der im vorigen Schritt registrierten App ein.

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

Sind alle erforderlichen Felder korrekt ausgefüllt, so wird die Schaltfläche „erstellen“ aktiviert.

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 – mit dem gleichen Zertifikat erstellen.

Um die Zertifikats-basierte Anmeldung von einem anderen Computer aus durchzuführen, kopieren Sie die zusammengehörigen *.pfx und *.o3s Dateien in das Verzeichnis „c:\data\office365checker\certs“ des entsprechende Computers. Die Anzeige in der Auswahlliste für Zertifikate erfolgt dann automatisch.

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.

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

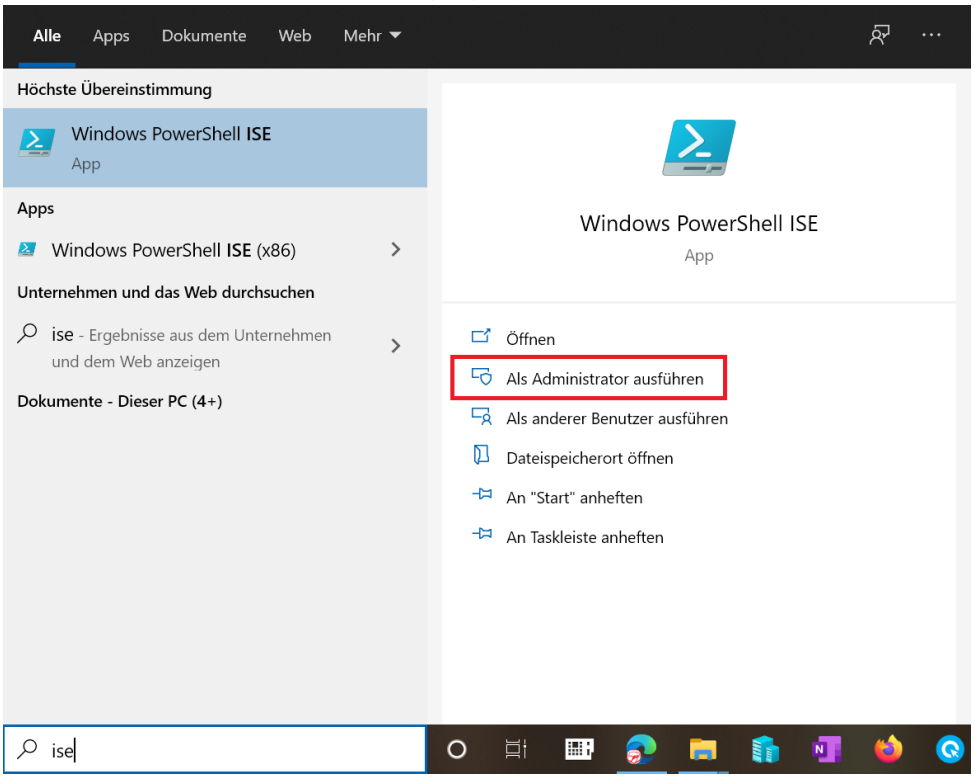
Das häufigste Problem im Umgang mit dem Microsoft 365 Checker tritt auf, wenn die Installation der PowerShell Module nicht ordnungsgemäß funktioniert.

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

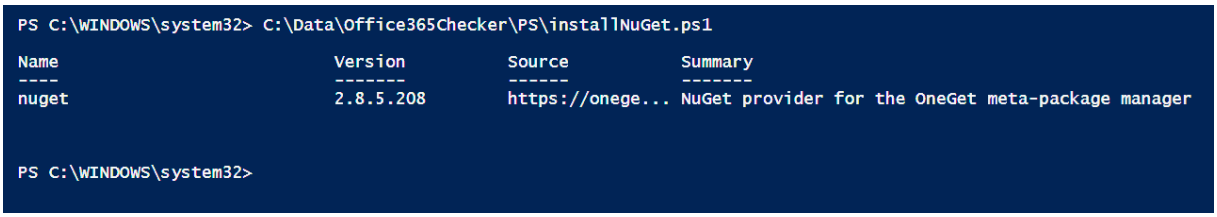


Geben Sie folgenden Befehl ein:

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.

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

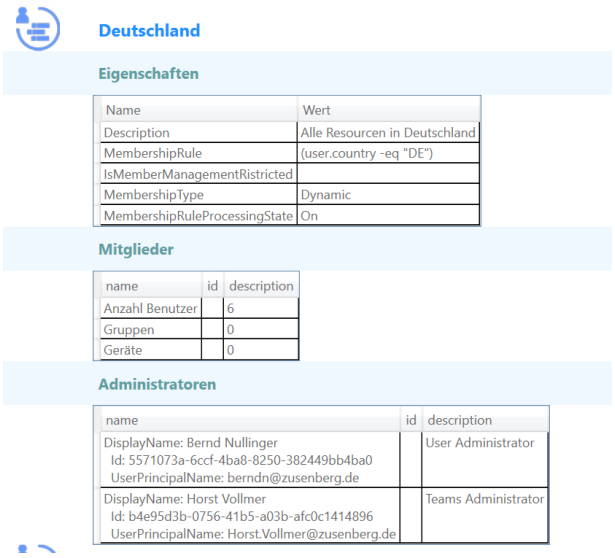
AAD Apps

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

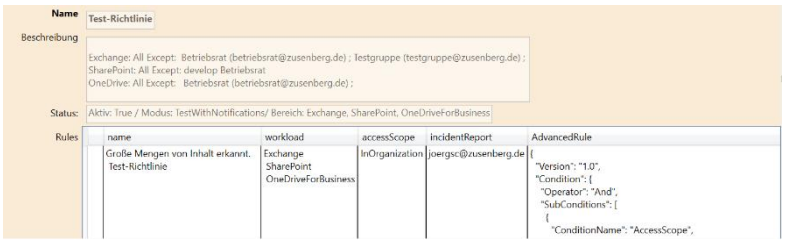
Alle verfügbaren Lizenzen mit:
Anzahl der verfügbaren Lizenzen
Anzahl der zugewiesenen Lizenzen

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

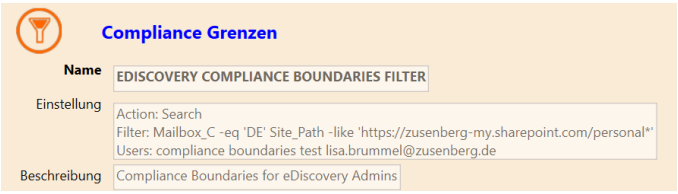
Hinweis: Um die Data Subject Requests auszulesen genügt die Rolle „Globaler Leser“ nicht!

Name
Beschreibung
Status
Erstellt am
Letzte Änderung von
Bearbeiter

Compliance Grenzen

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

Beispiel:



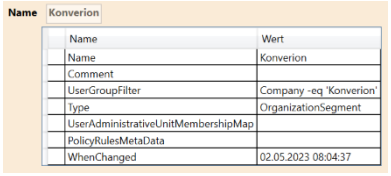
Die Compliance Grenze gilt für alle Benutzer aus der Gruppe „compliance boundaries test“, sowie für „lisa.brummel@zusenberg.de“.

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

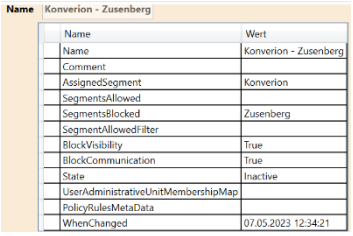
Über „Informations-Barrieren kann die Kommunikation zwischen definierten Benutzergruppen unterbunden werden /betrifft nur Chat und Freigaben, E-Mails können so nicht verhindert werden).

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

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

	in Verbindung mit E 5 Lizenzen und „Communication Compliance“ 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 Mögliche Werte: true / false
AllowMeetNow	Es können ad-hoc Besprechungen durchgeführt werden Mögliche Werte: true / false
AllowPrivateMeetNow	Es können private ad-hoc Besprechungen durchgeführt werden Mögliche Werte: true / false
MeetingChatEnabledType	Gibt an, ob Benutzer in Besprechungen chatten können. Mögliche Werte: Disabled, Enabled, EnabledExceptAnonymous
LiveCaptionsEnabledType	Live Untertitel in Besprechungen ermöglichen Mögliche Werte: Disabled / DisabledUserOverride
AllowIPVideo	Benutzer können in Besprechungen Video benutzen. Mögliche Werte: true / false
AllowAnonymousUsersToDialOut	Anonyme Benutzer können Festnetz-Anrufe tätigen. Mögliche Werte: true / false
AllowAnonymousUsersToStartMeeting	Anonyme Benutzer können Besprechungen starten. Mögliche Werte: true / false
AllowPrivateMeetingScheduling	Benutzer können privare Besprechungen planen. Mögliche Werte: true / false
AutoAdmittedUsers	Legt fest, wer die Besprechungslobby automatisch umgeht Mögliche Werte: EveryoneInCompany, EveryoneInSameAndFederatedCompany, Everyone, OrganizerOnly, EveryoneInCompanyExcludingGuests, InvitedUsers
AllowCloudRecording	Ermöglicht die Aufzeichnung von Besprechungen Mögliche Werte: true / false
AllowOutlookAddIn	Legt fest, ob Benutzer Besprechungen über den Outlook Client planen können. Mögliche Werte: true / false
AllowPowerPointSharing	Teilen von PowerPoint Präsentationen in Besprechungen erlauben. Mögliche Werte: true / false

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

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

VoiceIsolation	Gibt an, ob Benutzer die KI-unterstützte Geräuschunterdrückung in Besprechungen nutzen können. Mögliche Werte: enabled / disabled
EnrollUserOverride	Legt fest, ob Benutzer ihre Stimmprofile im Teams Client registrieren können. Mögliche Werte: enabled / disabled (Standard)
RoomAttributeUserOverride	Legt fest, ob Benutzer in Teams-Räumen aufgrund ihrer Stimme erkannt werden können. Mögliche Werte: **Off** Teams-Room Benutzer werden nicht erkannt. Die Stimmprofile der Benutzer werden nicht genutzt. **Attribute** Wenn Benutzer ihr Stimmprofil registriert haben, wird dieses genutzt um die Benutzer zu identifizieren und mit Namen zu versehen. **Distinguish** 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 Mögliche Werte: Enabled / Disabled
Description	Beschreibung der Richtlinie
EventAccessType	Legt fest, wer sich für Webinare registrieren kann. Mögliche Werte: Everyone – jeder kann sich registrieren, einschließlich Gäste und Externe EveryoneInCompanyExcludingGuest: es können sich nur Benutzer der eigenen Tenants registrieren
AllowTownHalls	Derzeit noch keine Auswirkung Mögliche Werte: Enabled / Disabled
AllowEmailEditing	Derzeit noch keine Auswirkung Mögliche Werte: Enabled / Disabled

Liveereignis-Richtlinien

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

Parameter	Bedeutung
AllowBroadcastScheduling	Benutzer können Live-Ereignisse planen Mögliche Werte: true / false
AllowBroadcastTranscription	Live-Ereignisse können transkribiert werden. Mögliche Werte: true / false
BroadcastAttendeeVisibilityMode	Legt fest, wer an Live-Ereignissen teilnehmen kann. Mögliche Werte: Everyone, EveryoneInCompany. InvitedUsersInCompany, EveryoneInCompanyAndExternal, InvitedUsersInCompanyAndExternal
BroadcastRecordingMode	Aufzeichnungs-Modus für Live-Ereignisse Mögliche Werte: 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 Mögliche Werte: enabled / disabled
EnrollFace	Benutzer können Gesichtsprofil registrieren 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. 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 Mögliche Werte: BlockedAppList, AllowedAppList
GlobalCatalogAppsType	Einstellung, ob die Liste der Drittanbieter- Apps die erlaubten, oder die blockierten Apps enthält Mögliche Werte: BlockedAppList, AllowedAppList
PrivateCatalogAppsType	Einstellung, ob die Liste der selbst erstellten Apps die erlaubten, oder die blockierten Apps enthält Mögliche Werte: 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
Copilot
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 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? Mögliche Werte: true/ false
IsCrossTenantDataMovementEnabled	Datenübertragung in anderen Tenant erlaubt? Mögliche Werte: true/ false
IsVivaInsightsEnabled	Viva Insights eingeschaltet? Bezieht sich nicht auf Viva Personal Insights, sondern das ehemalige Workplace Analytics Mögliche Werte: true/ false

Berichte

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

Parameter	Bedeutung

GraphApiEnabled	Zugriff per Graph-API erlaubt? Mögliche Werte: true/ false
PowerBiEnabled	Berichtsdaten für Power BI zur Verfügung stellen? Mögliche Werte: true/ false
PrivacyEnabled	Pseudonyme Bezeichner in allen Berichten verwenden? 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 Möglicher Werte: completed

Bookings

Parameter	Bedeutung
Enabled	Bookings für den gesamten Tenant ein-/ausschalten Mögliche Werte: true/ false
SocialSharingRestricted	Der „Mit Facebook verbinden“ Schalter wird entfernt
BookingsExposureOfStaffDetailsRestricted	Es werden keine Mitarbeiterdaten in der Kommunikation mit Kunden versendet Mögliche Werte: true/ false
StaffMembershipApprovalRequired	Benutzer müssen die Freigabe ihres Kalenders in Bookings beantragen und als Mitarbeiter in Bookings eingetragen werden Mögliche Werte: true/ false
BookingsSmsMicrosoftEnabled	Microsoft kann SMSe zur Terminbestätigung an Kunden versenden Mögliche Werte: true/ false
BookingsSearchEngineIndexEnabled	Verhindert, dass die Buchungsseiten von Bookings in Suchergebnissen von Bing oder Google auftauchen Mögliche Werte: true/ false
BookingsNamingPolicyEnabled	Namenskonventionen für die Bookings-Kalender durchsetzen 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 Mögliche Werte: true/fasle
ExternalSendFormEnabled	Externen kann ein Link zum Formular gesendet werden, um Antworten zu sammeln Mögliche Werte: true/fasle
ExternalShareCollaborationEnabled	Formular kann gemeinsam mit Externen bearbeitet werden 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 Mögliche Werte: true/false
RecordIdentityByDefaultEnabled	Namen standardmäßig erfassen Mögliche Werte: true/false
BingImageSearchEnabled	Das Hinzufügen von Bildern von Bing und aus YouTube-Videos in Forms gestatten
InOrgFormsPhishingScanEnabled	Internen Schutz vor Pishing aktivieren 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. 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. Mögliche Werte: true/false

MyAnalytics

Diese Einstellungen gelten für alle Benutzer.

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

Elementeinblicke

Parameter	Bedeutung
AllowItemInsights	Elementeinblicke für alle Benutzer einschalten (Wenn die Elementeinblicke generell erlaubt sind, können sie von jedem Benutzer in seinen Datenschutzeinstellungen abgeschaltet werden) Mögliche Werte: true/false
DisabledForGroup	Die Elementeinblicke sind für bestimmte Benutzergruppen abgeschaltet. 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 Mögliche Werte: true/false

Integrated Apps Settings

Standardeinstellungen für Integrierte Apps (ersetzt im Laufe der Zeit die App-Einstellungen aus Teams)

Parameter	Bedeutung
areFirstPartyAppsAllowed	Alle Microsoft Apps erlaubt Mögliche Werte: true/false
areThirdPartyAppsAllowed	Alle 3rd Party Apps erlaubt Mögliche Werte: true/false
areLOBAppsAllowed	Alle Mandanten-Apps Mögliche Werte: true/false
CopilotExtensibilitySettings	
isCopilotExtensibilityApplicable	Copilot Agenten erlaubt Mögliche Werte: true/false
userAssignmentCategory	Wer darf Agenten nutzen Mögliche Werte: everyOne -> jeder NoOne -> niemand SpecifiedUsers - > bestimmte Benutzer
members	Wenn userAssignmentCategory = SpecifiedUsers ist hier die Liste der zugelassenen Benutzer und Gruppen

Viva Modules

Liste der im Tenant vorhandenen Viva Module

Beispiel

Name	Plan	Admin
Viva Learning	Add-On, In Microsoft 365	Name des Adminstrators (falls vorhanden)

Name entspricht dem Namen des Viva Moduls

Plan kann „Add-On“ sein, wenn eine separate Lizenz erworben wurde, „In Microsoft 365“, wenn es kostenloser Bestandteil der Microsoft 365 Lizenz ist, oder beides, wenn zu der kostenlosen Lizenz die kostenpflichtige Version hinzugebucht wurde

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“.

Copilot

Lizenzen

Übersicht über die gekauften und zugewiesenen Copilot Premium Lizenzen

name	accountSkuId	availableUnits	totalUnits	consumedUnits
Microsoft 365 Copilot	expertenrunde:Microsoft_365_Copilot	0	2	2

Available Units ist die Anzahl der noch nicht zugewiesenen Lizenzen

totalUnits ist die Anzahl der im Tenant vorhandenen (gekauften) Lizenzen

consumedUnits ist die Anzahl der zugewiesenen Lizenzen

Copilot Selbstbedienungseinkäufe

Benutzer können Copilot Premium Lizenzen selbst mit ihrem Unternehmenskonto kaufen und sie mit einer privaten Kreditkarte bezahlen.

Parameter	Bedeutung
Product	Produktbezeichnung
Setting	Mögliche Einstellungen: enabled - verfügbar disabled – nicht verfügbar OnlyTrialsWithoutPaymentMethod – nur Produkte, für die keine Zahlung (per privater Kreditkarte . erforderlich ist

Flex Routing

Copilot Anfragen können bei Lastspitzen auch in Rechenzentren außerhalt der Europäischen Union verarbeitet werden. Es werden nie Daten außerhalb der EU gespeichert.

Parameter	Bedeutung
effectiveValue	Mögliche Werte: True – Flex Routing ist erlaubt False – Flex Routing ist deaktiviert
adminOverride	Derzeit noch nicht in Verwendung, Standardwert: „NotSet“

Teams

Verfügbarkeit von Copilot in Teams Besprechungen

Parameter	Bedeutung
AllowTranscription	Transkription erlaubt Mögliche Werte: True / False
Copilot	Verfügbarkeit von Copilot in Teams Besprechungen.

	Mögliche Werte: On – Copilot ist verfügbar EnabledWithTranscript – Copilot ist nur verfügbar, wenn ein gespeichertes Transkript vorhanden ist EnabledWithTranscriptDefaultOn – Copilot ist in Besprechungen verfügbar und das Transkript wird automatisch gespeichert Off – Copilot ist in Teams Besprechungen nicht verfügbar

Copilot in Víva

Verfügbarkeit von Copilot in Viva Insights.

Standardmäßig ist Copilot für alle lizensierten Benutzer in Viva Insights verfügbar („Default Policy“). Über Richtlinien kann die Verfügbarkeit entweder nur für bestimmte Benutzer freigegeben werden („On for specific people“) oder für bestimmte Benutzer abgeschaltet werden („Off for specific people“)

Parameter	Bedeutung
Name	Name der Richtlinie. Standard „Default Policy“
Policy Id	Wenn eine benutzerdefinierte Richtlinie eingerichtet wurd3e, die Objekt-Id der Richtlinie
FeatureId	CopilotInVivaInsights
ModifiedOn	Datum der letzten Änderung. Ohne benutzerdefinierte Richtlinie immer „01.01.0001 00:00:00“
CreatedOn	Datum der Erstellung. Ohne benutzerdefinierte Richtlinie immer „01.01.0001 00:00:00“
IsFeatureDisabled	Funktion ausgeschaltet Mögliche Werte: True / False
IsUserControlEnabled	Funktion ist verfügbar, aber Benutzer müssen sich anmelden
IsUserOptedInByDefault	Funktion ist für alle Benutzer verfügbar verfügbar, Benutzer müssen sich bei Bedarf abmelden

Admin Center

Einstellung, ob Copilot in Admin Centern erlaubt ist.

Parameter	Bedeutung
PolicyConfigurationId	LgAAAABnHf9IV1WMRIe-09RzNAs5AQB_nwewrr9VSqJMbqK7n65TAAL2OBjXAAAB0 Dies sit die Standard-Id. Sie ist immer gleich.
CopilotToggleSettingPolicy	Feld ist leer, wenn alle Admins Copilot in Admin Centern nutzen können. Der Wert ist 0, wenn Copilot für alle Admin Center deaktiviert ist.

Video Generierung

KI-unterstütztes Erstellen von Videos erlauben.

Relevant ist lediglich der Wert des Parameters „Policy“. Ist dieser 0, ist das KI-gestützte Erstellen von Videos erlaubt. Ansonsten ist der Wert 1.

Parameter	Wert / Bedeutung
Name	CopilotBlockVideoGeneration
SettingId	office16;L_CopilotBlockVideoGeneration
IsDefaultPolicy	False
PolicyConfigurationId	LgAAAABnHf9IV1WMRIe-09RzNAs5AQB_nwewrr9VSqJMbqK7n65TAAL2OBjXAAAB0
TargetTenantPolicyConfigurationId	
PolicyConfigurationGroupIds	
Policy	**0** Wenn der Wert 0 ist, ist das Erstellen von Videos erlaubt, ansonsten ist der Wert 1
DefaultPolicyValue	0
ChildSettingPolicy	
ManageInOCPS	False
PolicyAssignmentType	3
TargetTenantPolicyAssignmentType	
GroupPolicyCount	1
VisibleTenantPolicyCount	1
HiddenTenantPolicyCount	0

Bild Generierung

Einstellung, ob das KI-gestützte Erstellen von Bildern erlaubt ist.

name	value
PolicyConfigurationId	LgAAAABnHf9IV1WMRIe-09RzNAs5AQB_nwewrr9VSqJMbqK7n65TAAL2OBjXAAAB0
CopilotImageGenerationPolicy	Wenn dieses Feld leer ist, ist das Erstellen von Bildern erlaubt, sonst ist der Wert 1

3rd Party Modelle

Liste der verfügbaren KI-Modelle. Derzeit außerhalb der USA nur Anthropic möglich.

Parameter	Wert Bedeutung
DisplayName	Anthropic
EnabledForAllUsers	True Anthropic ist verfügbar, ansonsten wäre der Wert False
Entities	[]

Description	AI safety and research company.
IsConfigured	True Wenn Anthropic nicht freigegeben ist, ist dieser Wert False
Identifier	P_bbef1ffa-25db-4bb9-870d-afb22f41a4e9
ModifiedBy	fa01c802-e095-43d4-ba14-76f03aaf6679 Benutzer-ID des Administrators, der Anthropic freigegeben hat
ModifiedDate	17.04.2026 05:03:09 Datum und Uhrzeit (UTC) der Freigabe

Frontier

Frontier ist das Early-Access Programm für KI-Funktionen.
Frontier ist – wie alle Vorschauversionen – von dem Datenschutznachtrag zu den Produktbestimmungen ausgeschlossen.

Es können bis zu 10.000 Benutzer in das Programm eingetragen werden.

Parameter	Wert / Beschreibung
PolicyConfigurationId	8e81c383-5dc4-4c6e-9ddb-c52ee1fae5f9
FrontierPolicy	1
GroupIds	[] Liste der Gruppen, die im Frontier Programm sind
UserIds	["1a72379b-581a-416f-a76d-d387595a8dd9"] Liste der Benutzer, die im Frontier Programm sind
AudienceStatus	PartiallyEnrolled – wenn Benutzer im Programm sind NotEnrolled – wenn keine Benutzer für Frontier registriert sind

Capacity	{
	"limit": 10000,
	"estimatedTotalAssignments": 1,
	"isLimitExceeded": false
	}

Opal

Opal (derzeit nur im Frontier-Programm verfügbar) ist ein KI-Agent, der eigenständig Aufgaben auf einem Cloud-PC ausführen kann (Get started with Project Opal (Frontier) | Microsoft Support)

Parameter	Wert / Beschreibung
allowedOnboardingUsersAndGroups	[] Benutzer und Gruppen, die sich für Opal registrieren können
allowedOnboardingUsersCategory	NoOne Benutzerkategorien, die sich für Opal registrieren können

isDeployed	False Opal ist nicht im Tenant verfügbar, sonst True
isDeployedForEveryone	False Opal ist nicht für alle Benutzer verfügbar, sonst True
assignedUsersAndGroups	[]
allowedUsersAndGroups	[]
allowedUsersCategory	Everyone