Microsoft

Microsoft Security für Remotemitarbeiter.

Schnell, aber überlegt.

Für Microsoft-Kunden.

Wenn Sie wie Microsoft plötzlich eine hauptsächlich heimbasierte Belegschaft unterstützen müssen, möchten wir Ihnen dabei helfen, sicherzustellen, dass Ihre Organisation so sicher wie möglich arbeiten kann. In diesem Dokument werden Aufgaben und Themen vorgestellt, mit denen Sicherheitsteams wichtige Sicherheits- und Verwaltungsfunktionen so schnell wie möglich implementieren können.

Folgende Personen der Microsoft Deutschland GmbH haben zur Erstellung dieses Dokuments beigetragen:

Idee und Umsetzung
Andreas Mangerich – Technical Specialist Cyber Security & Compliance

Technische Beratung, inhaltliche Ausarbeitung und Rezension
Stephanus Schulte – Cloud Solution Architect
Hermann Maurer – Technical Specialist Cyber Security & Compliance
Holger Zimmermann – Technical Specialist Cyber Security & Compliance
Sebastian Meiforth – Partner Technical Architect

Inhalt

Erste Schritte

Unterstützung durch Microsoft FastTrack

FastTrack erleichtert Kunden die Bereitstellung von Microsoft Cloud-Lösungen. Kunden mit berechtigten Abonnements für Microsoft 365, Azure oder Dynamics 365 können FastTrack während der Laufzeit ihres Abonnements ohne Zusatzkosten nutzen.

Die FastTrack-Dienste finden Sie hier: https://www.microsoft.com/de-de/fasttrack?rtc=1

Erstellung einer Mandantenumgebung (Tenant)

Dies erfolgt in der Regel durch den Microsoft-Partner/IT-Dienstleister, sobald die Lizenzen gebucht werden.

Wenn bereits ein Microsoft Cloud-Service genutzt wird, ist der Tenant schon vorhanden. Sollte dies nicht der Fall sein, dann wird der Tenant vom Dienstleister (CSP-Partner oder Distributor) als Voraussetzung für das Hinzubuchen der (Trial-) Lizenzen oder automatisiert beim Beantragen der Trial-Lizenzen erstellt.

Wichtige Information: Wenn Ihre Organisation keine Identitäten mit Azure Active Directory (Azure AD) synchronisiert hat, lesen Sie Identitätsmodelle und Authentifizierung in Microsoft Teams.

Lizenzen

Folgende Liste gibt eine Übersicht über in diesem Dokument behandelte Lösungen sowie entsprechende Lizenzierungsoptionen. Dabei können diese Lösungen auch oftmals einzeln lizenziert werden. Details hierzu erhalten Sie von Ihrem CSP- oder Microsoft-Vertriebskontakt.

Tabelle 1: Lizenzübersicht

Sicherheitsaufgabe	**Azure AD Premium Plan 1**	**Enterprise Mobility + Security E3**	**M365 E3**	**M365 E5** (**Security**)
Azure-basierte Multi-Faktor-Authentifizierung (MFA)	✓	✓	✓	✓
Conditional Access	✓	✓	✓	✓
Self-Service Password Reset (SSPR)	✓	✓	✓	✓
Azure Application Proxy	✓	✓	✓	✓
Dynamische Gruppenmitgliedschaften	✓	✓	✓	✓
Gruppenbasierte Lizenzierung	✓	✓	✓	✓
VPN Split-Tunneling		✓	✓	✓
Microsoft Intune		✓	✓	✓
Mobile Device Management		✓	✓	✓
Office 365 Advanced Threat Protection (ATP) (externer Link)			✓	✓
Azure Advanced Threat Protection (ATP) (externer Link)				✓
Microsoft Cloud App Security (externer Link)				✓
Microsoft Defender Advanced Threat Protection (ATP, inkl. EDR) (externer Link)				✓

Benutzerverwaltung und Lizenzzuweisung

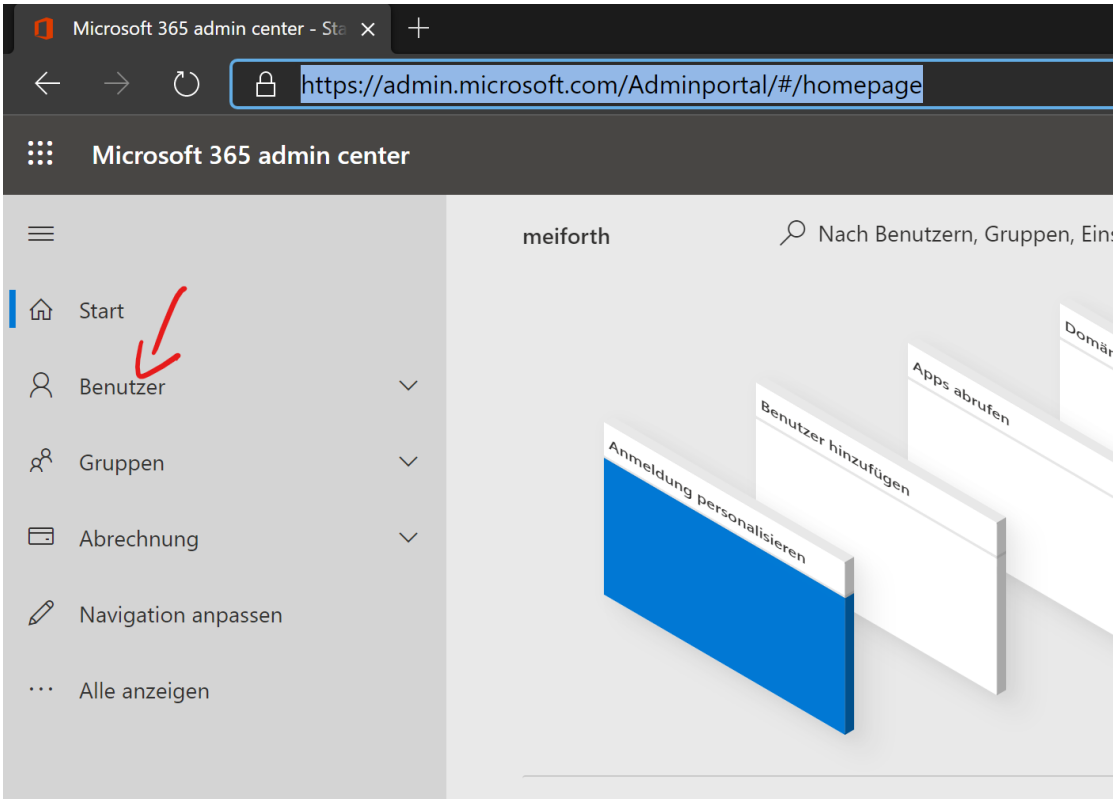
In der Basic Benutzerverwaltung zeigen wir auf, wie schnell Benutzer über die Portale angelegt und Lizenzen zugewiesen werden können. – Ideal für kleine Unternehmen, die keinen Domain Controller (Server für die Identitäts- und Rechteverwaltung) im Einsatz haben.

Hinzufügen oder Löschen von Benutzern in Azure Active Directory

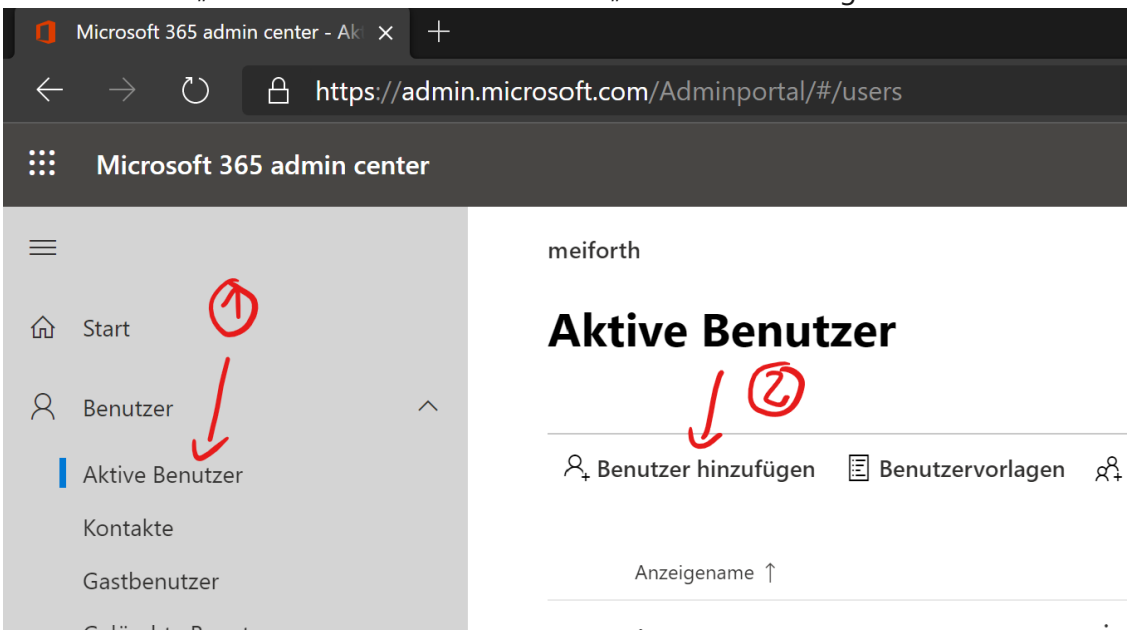
Sie können Ihrer Azure Active Directory-Organisation neue Benutzer hinzufügen oder vorhandene Benutzer aus der Azure AD-Organisation löschen. Sie müssen ein Benutzeradministrator oder globaler Administrator sein, um Benutzer hinzufügen oder löschen zu können. Natürlich können Benutzer und Gruppen auch über andere Portale, wie zum Beispiel das Office/Microsoft 365 Admin Center (wie hier im „Basic" Guide gezeigt), hinzugefügt werden.

Hinzufügen eines neuen Benutzers plus Lizenz (Basic) im Microsoft/Office 365 Admin Portal

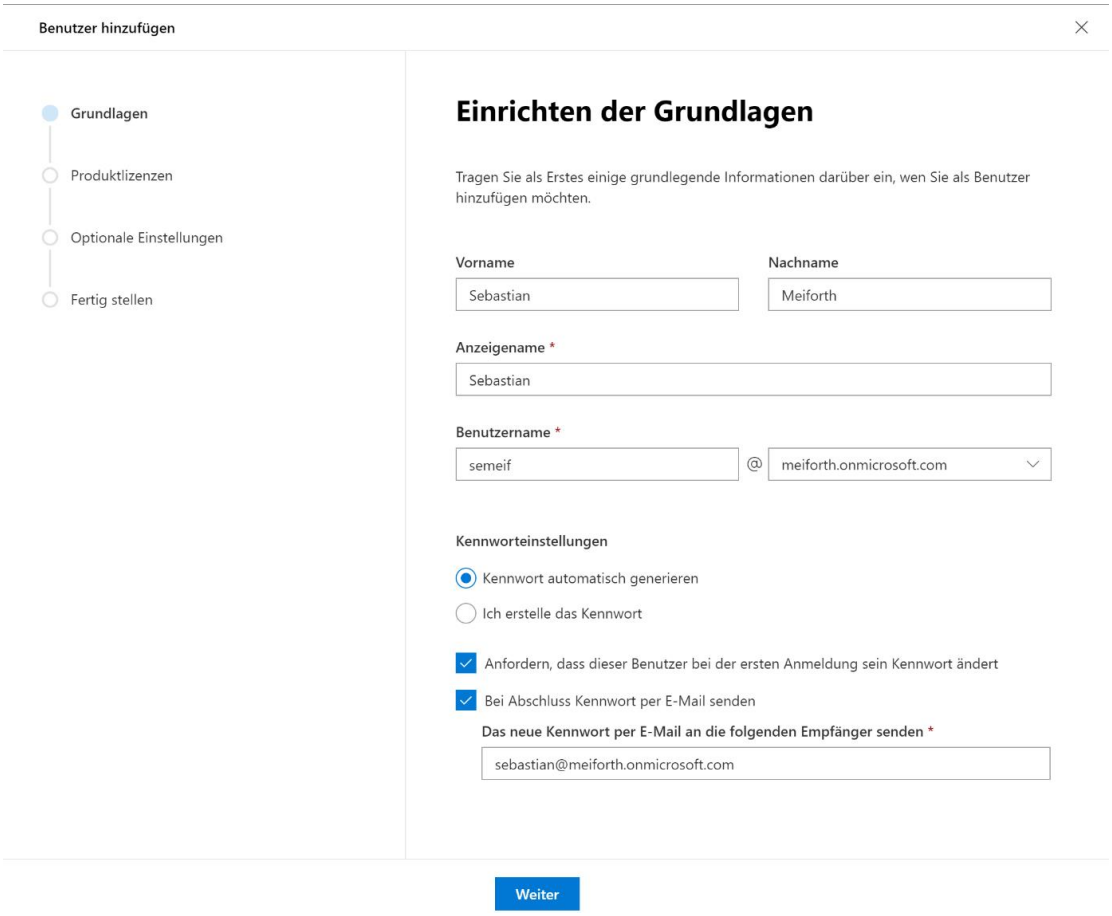
1. Öffnen Sie das Admin Portal: https://admin.microsoft.com/Adminportal/#/homepage
2. Erweitern Sie das Menü „Benutzer".



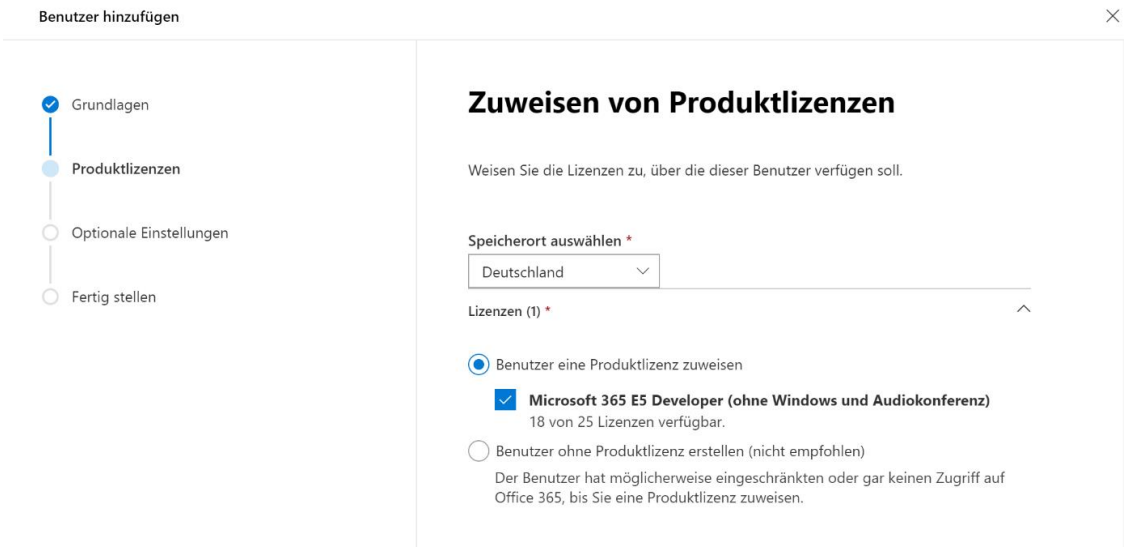
3. Klicken Sie auf „Aktive Benutzer“ und dann auf „Benutzer hinzufügen“.



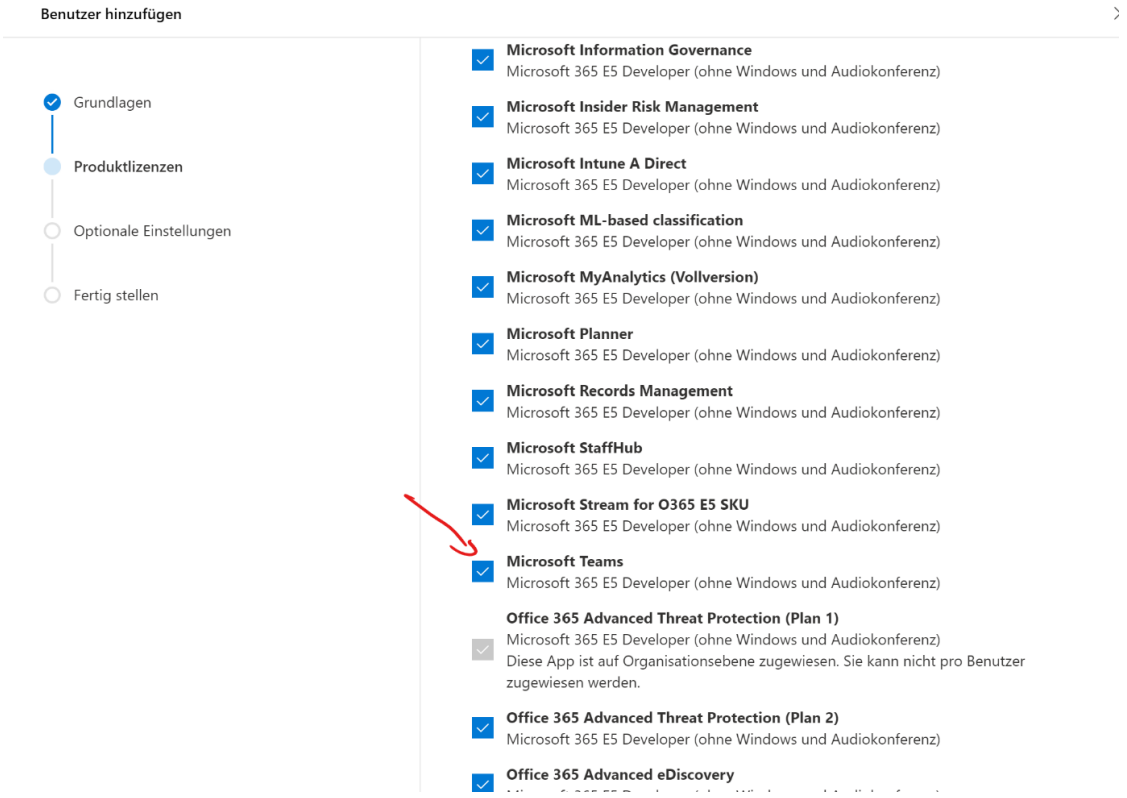
4. Geben Sie die Benutzerinformationen ein und klicken Sie auf „Weiter“.



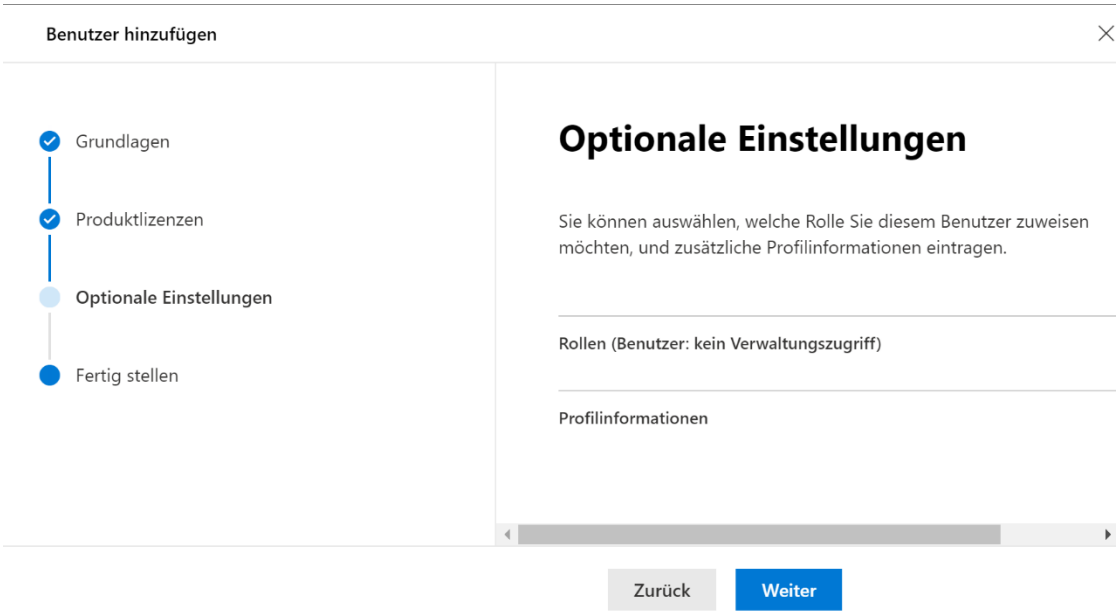
5. Weisen Sie dem Nutzer die entsprechende (Teams-) Lizenz zu und wählen Sie den „Speicherort“ aus.



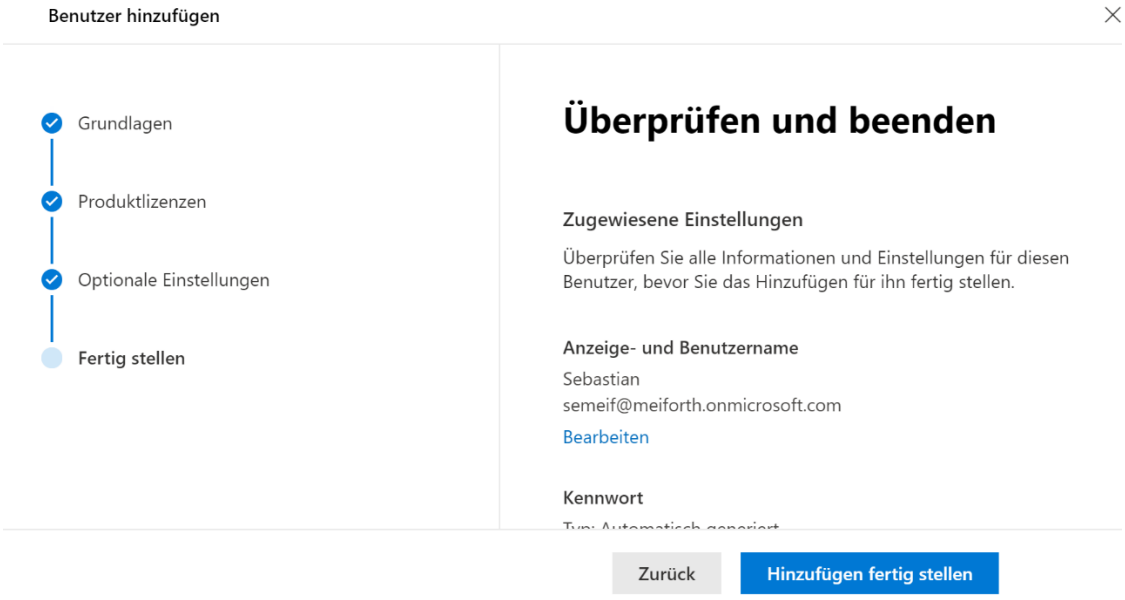
6. Erweitern Sie auf der gleichen Seite das Menü „Apps“ und stellen Sie sicher, dass „Microsoft Teams“ ausgewählt ist, und klicken Sie dann auf „Weiter“. (Die angezeigten Apps weichen je nach ausgewählter Lizenz ab!)



7. Klicken Sie auf „Weiter“.

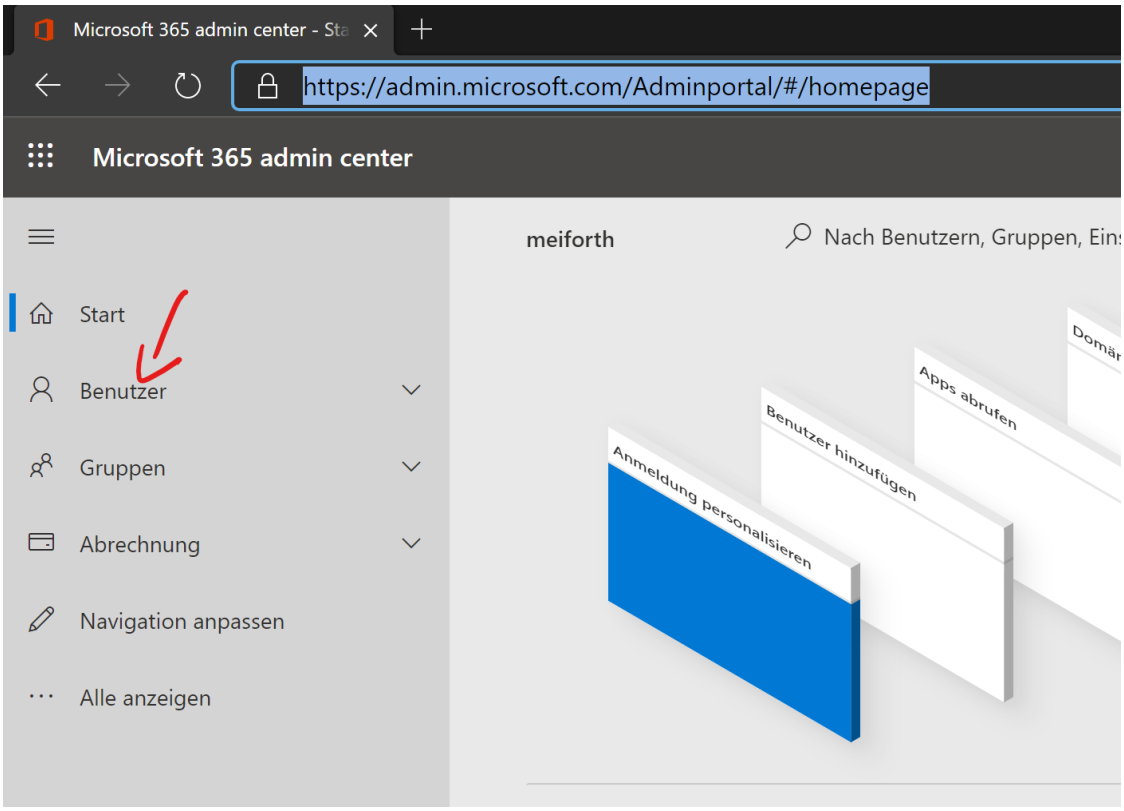


8. Klicken Sie auf „Hinzufügen fertig stellen“.

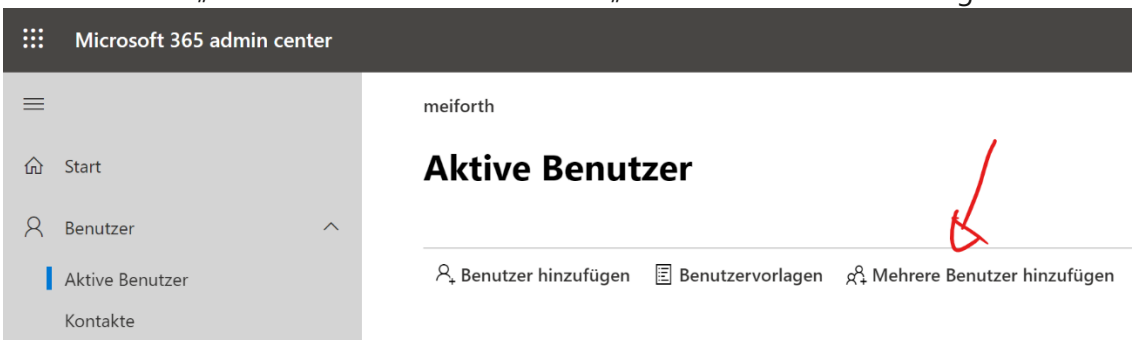


Mehrere Benutzer (Bulk)

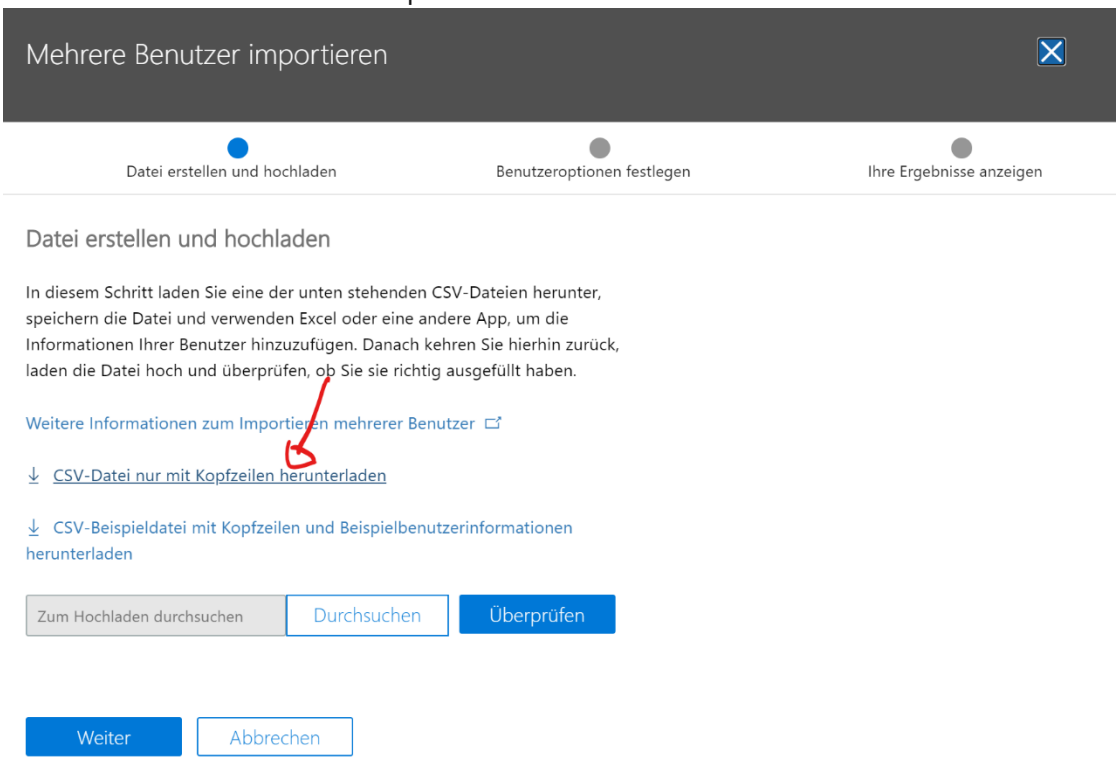
1. Öffnen Sie das Admin Portal: https://admin.microsoft.com/Adminportal/#/homepage
2. Erweitern Sie das Menü „Benutzer“.



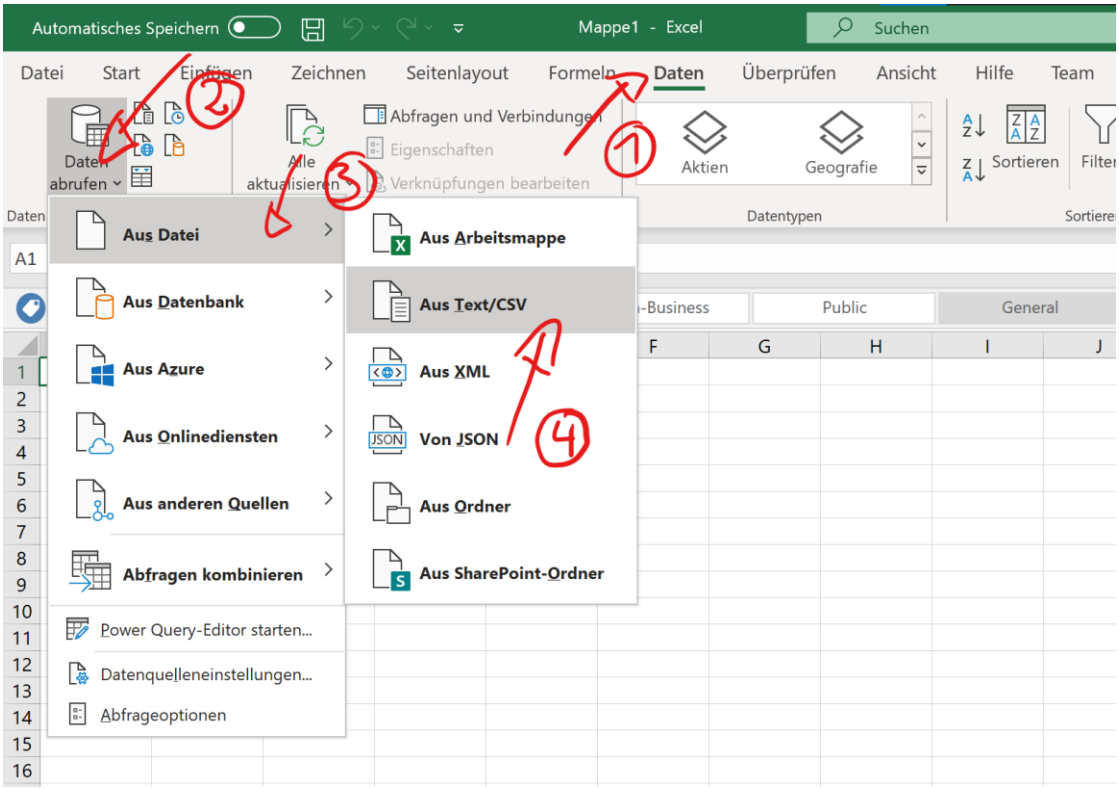
3. Klicken Sie auf „Aktive Benutzer“ und dann auf „Mehrere Benutzer hinzufügen“.



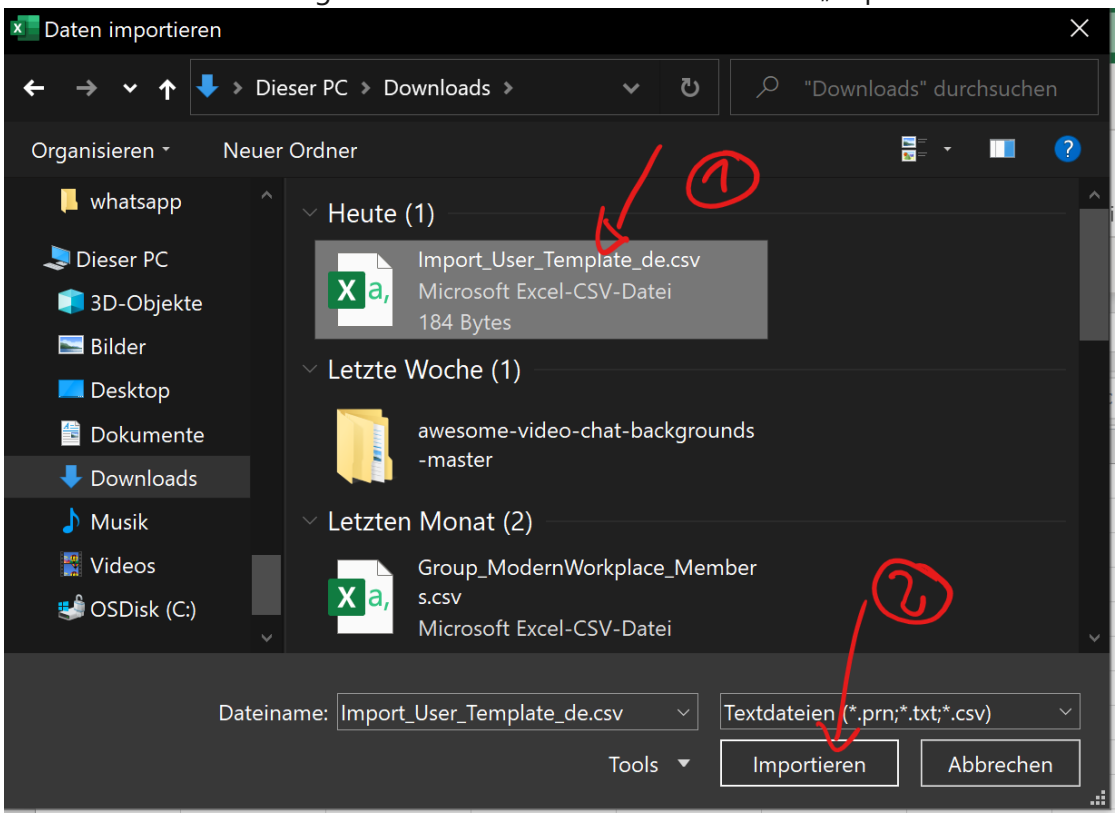
4. Laden Sie die CSV-Datei mit Kopfzeilen herunter.



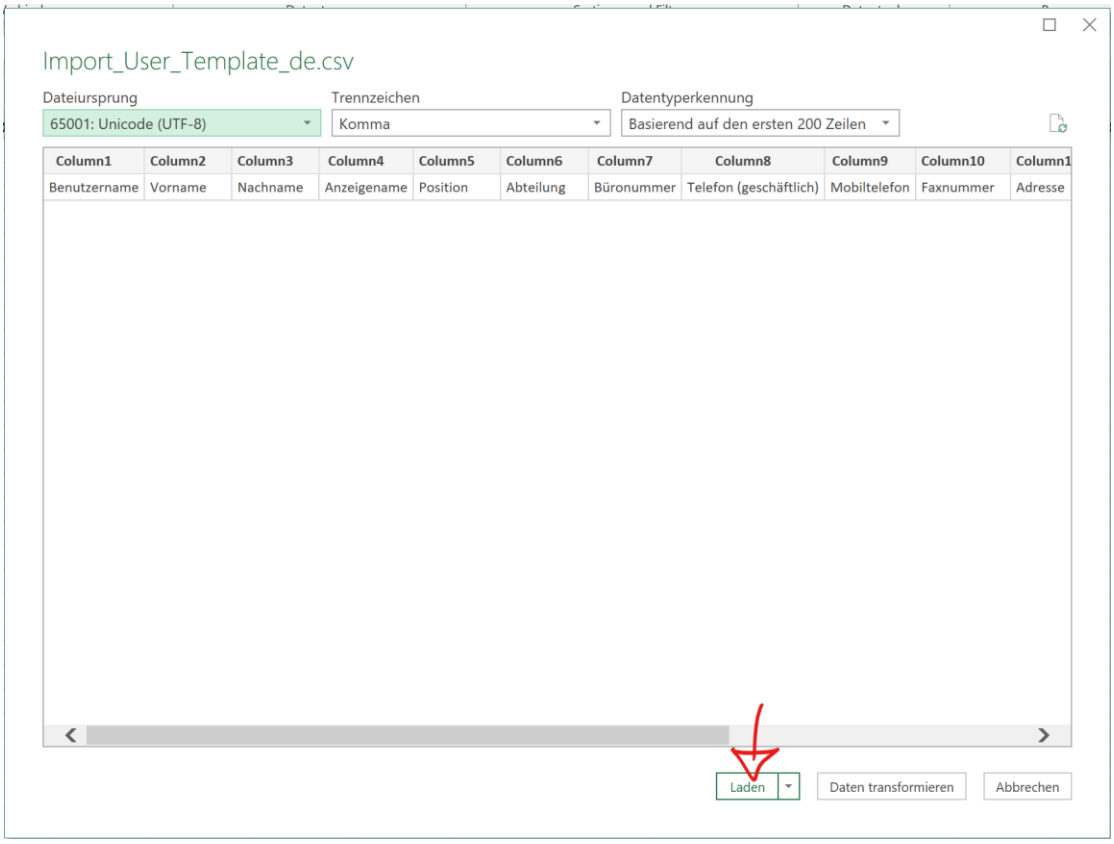
5. Öffnen Sie die CSV-Datei in Excel. Öffnen Sie dazu den Menüpunkt „Daten" → „Daten abrufen" → „Aus Datei" → Aus „Text/CSV".



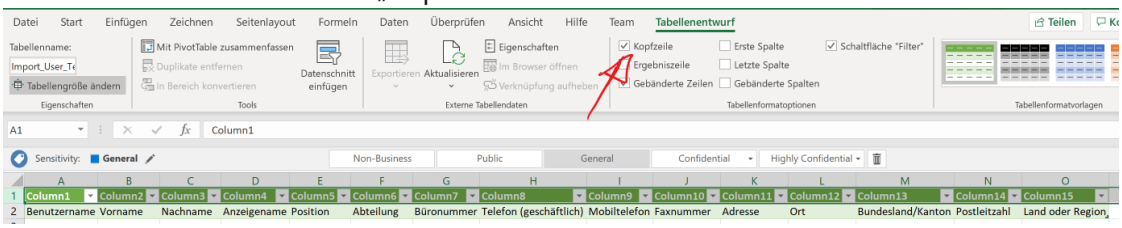
6. Wählen Sie die heruntergeladene Datei aus und klicken Sie auf „Importieren“.



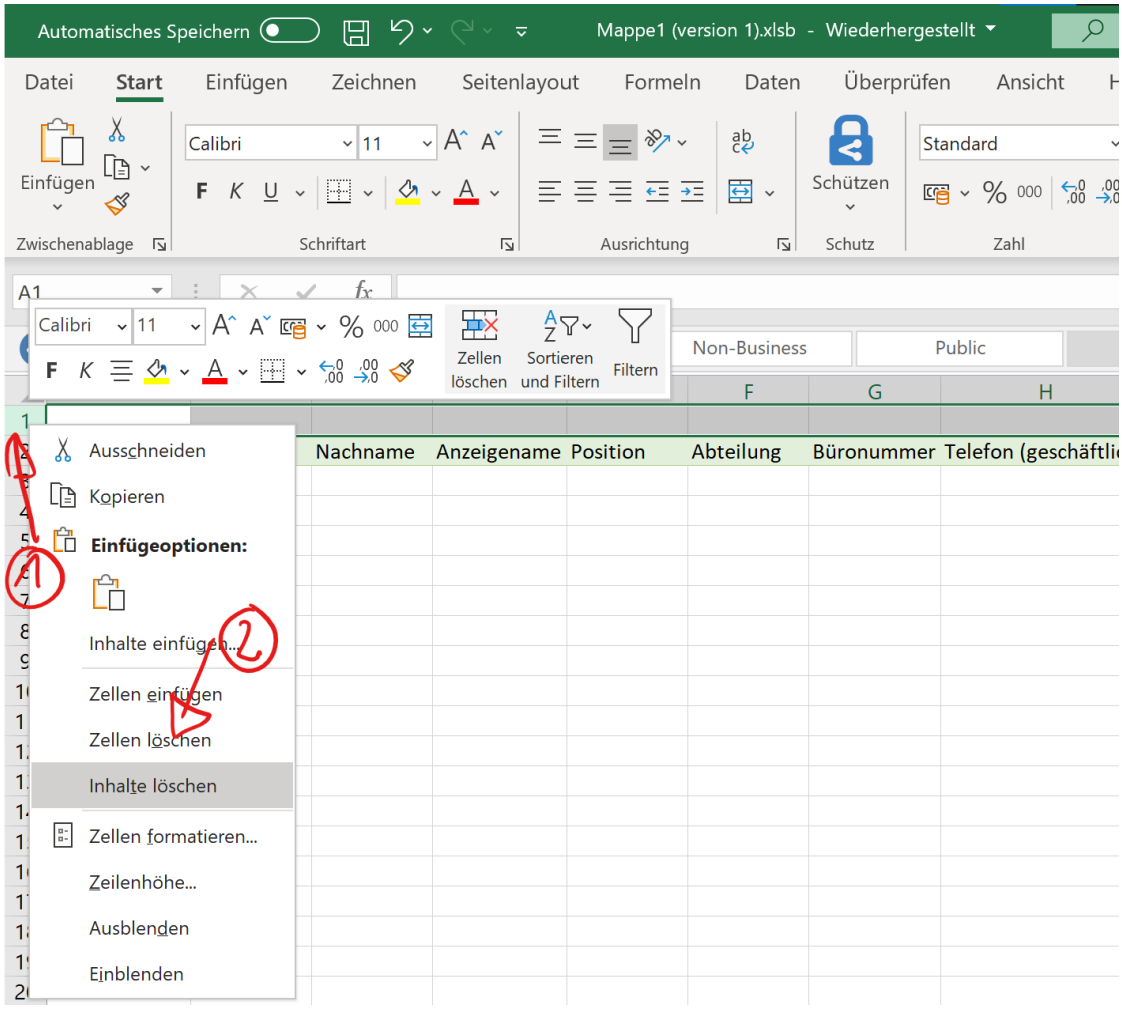
7. Klicken Sie auf „Laden“.



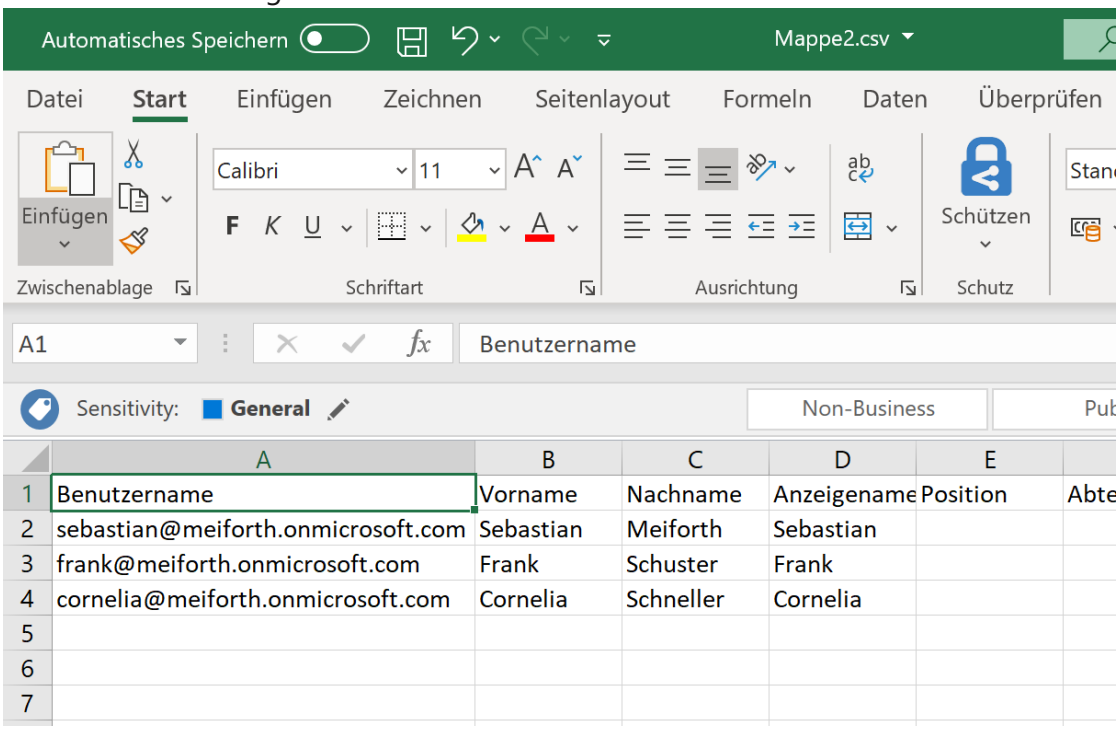
8. Entfernen Sie den Haken bei „Kopfzeile“.



9. Markieren Sie die erste Zeile, klicken Sie mit der rechten Maustaste davor und dann auf „Zellen löschen“.

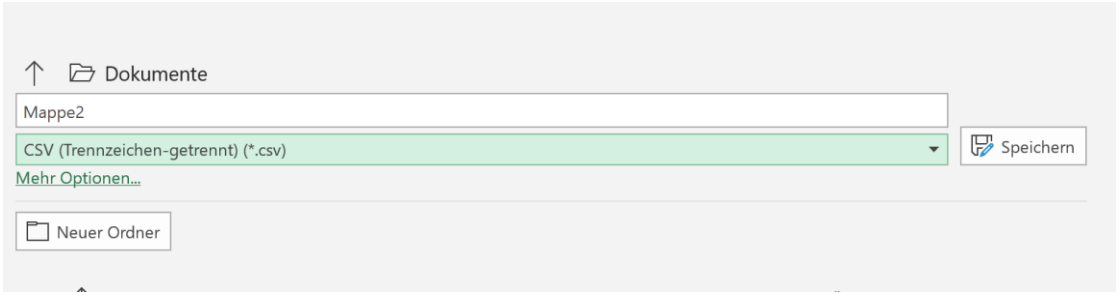


10. Füllen Sie die benötigten Felder aus.

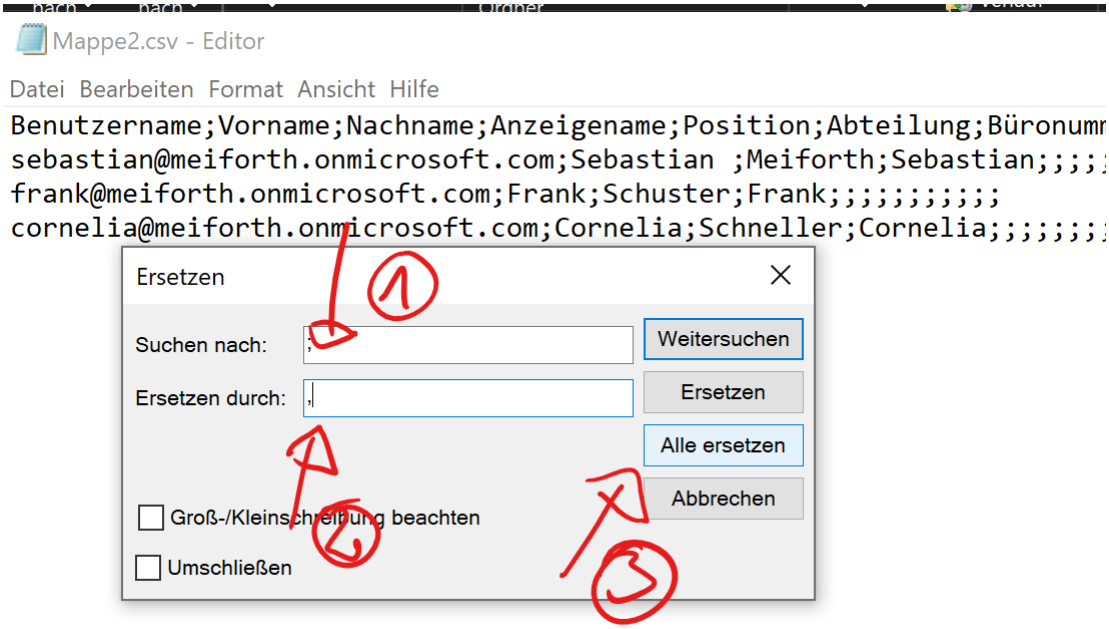


	A	B	C	D	E	
1	Benutzername	Vorname	Nachname	Anzeigename	Position	Abte
2	sebastian@meiforth.onmicrosoft.com	Sebastian	Meiforth	Sebastian		
3	frank@meiforth.onmicrosoft.com	Frank	Schuster	Frank		
4	cornelia@meiforth.onmicrosoft.com	Cornelia	Schneller	Cornelia		
5						
6						
7						

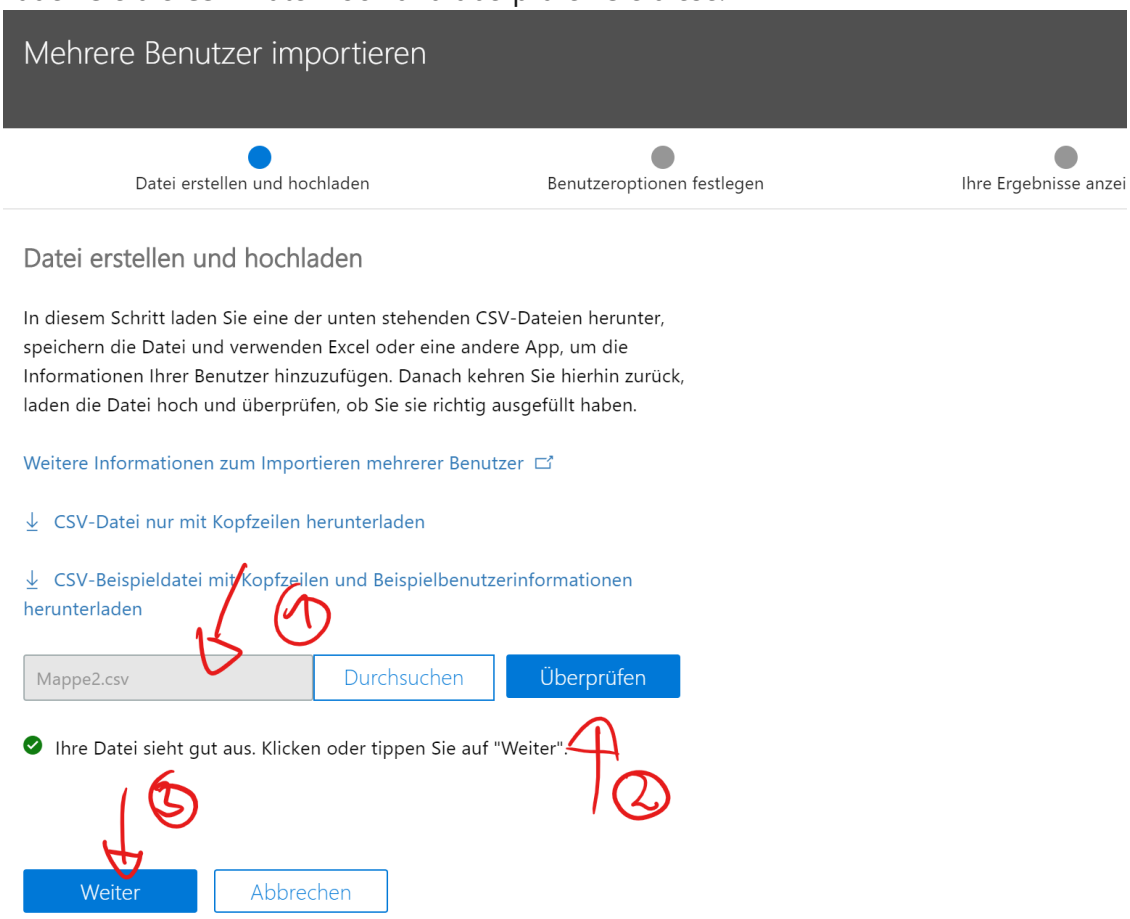
11. Speichern Sie das Dokument wieder als CSV.



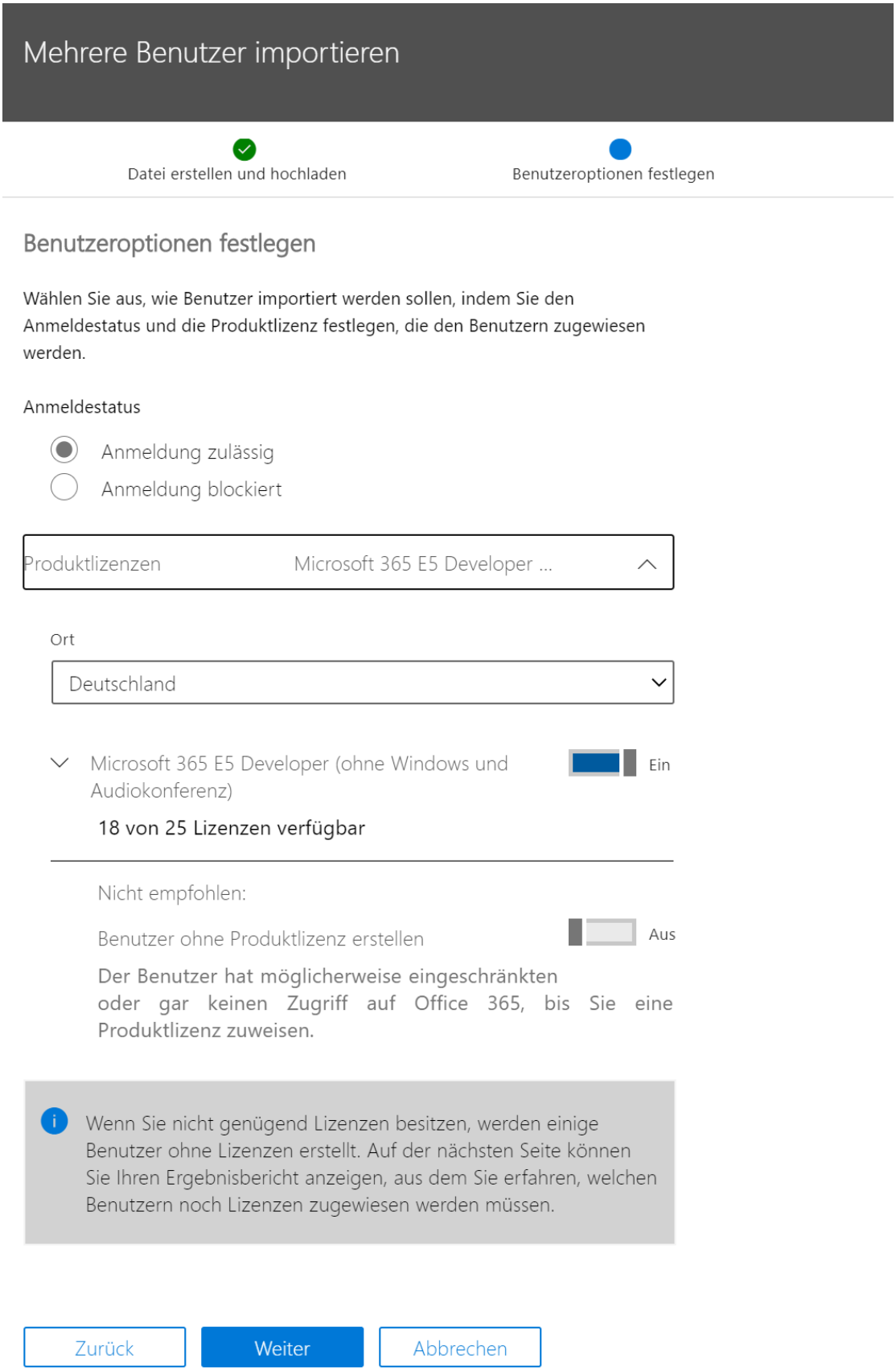
12. **Achtung!** In Europa wird das Semikolon zur Zeilentrennung verwendet. Der Upload erfordert aber ein Komma. Daher bitte im Editor suchen und ersetzen:



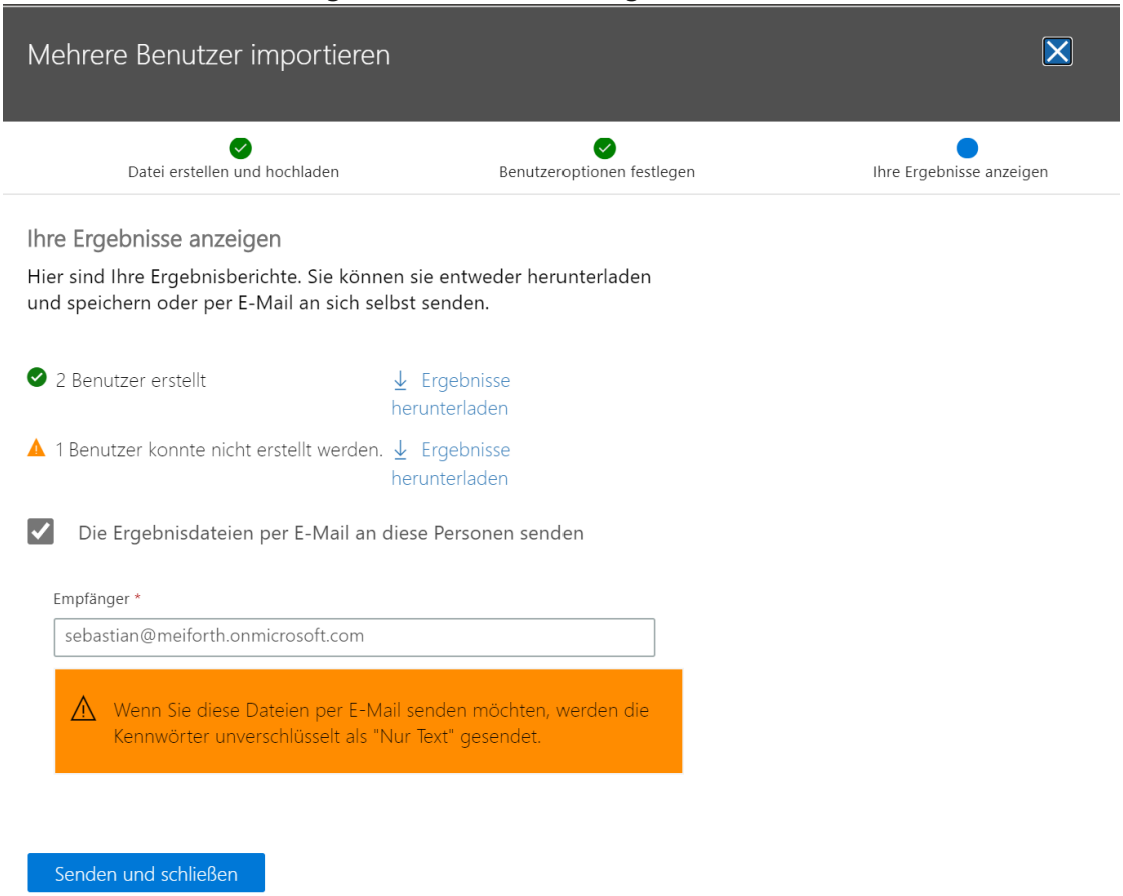
13. Laden Sie die CSV-Datei hoch und überprüfen Sie diese.



14. Weisen Sie die Lizenzen zu.



15. Nun werden die Nutzer erstellt und Sie haben die Möglichkeit, gleich die Passwörter zu versenden. Achtung: Dies erfolgt unverschlüsselt. Sollten Fehler auftreten, zum Beispiel doppelte Benutzernamen, bekommen Sie hier ebenfalls gleich die Info. Die Passwörter können auch gleich als CSV heruntergeladen werden.



Dokumentbeginn

Azure Active Directory Premium P1

Grundlegendes zu Identitäten in Azure Active Directory

Office 365 verwendet Azure Active Directory (Azure AD), einen cloudbasierten Benutzeridentitäts- und Authentifizierungsdienst, der in Ihrem Office 365-Abonnement enthalten ist, um Identitäten und Authentifizierung für Office 365 zu verwalten. Die ordnungsgemäße Konfiguration Ihrer Identitätsinfrastruktur ist entscheidend für die Verwaltung des Office 365-Benutzerzugriffs und der Berechtigungen für Ihre Organisation.

Um Benutzerkonten zu planen, müssen Sie zunächst die beiden Identitätsmodelle in Microsoft 365 verstehen. Sie können die Identitäten Ihrer Organisation nur in der Cloud verwalten, oder Sie können Ihre lokalen AD DS-Identitäten (Active Directory Domain Services) verwalten und diese zur Authentifizierung verwenden, wenn Benutzer auf Microsoft 365-Clouddienste zugreifen sollen.

Nachfolgend finden Sie die beiden Identitätstypen sowie deren beste Anwendungsfälle und Vorteile:

Tabelle 2: Vergleich der Identitätstypen

	Reine Cloudidentität	**Hybrididentität**
Definition	Ein Benutzerkonto ist nur im Azure Active Directory-Mandanten (Azure AD) für Ihr Microsoft 365-Abonnement vorhanden.	Ein Benutzerkonto ist in AD DS vorhanden, und eine Kopie befindet sich auch im Azure AD-Mandanten für Ihr Microsoft 365-Abonnement. Das Benutzerkonto in Azure AD enthält möglicherweise auch eine Hashversion des Kennworts für das Benutzerkonto.
Authentifizierung von Benutzeranmeldeinformationen durch Microsoft 365	Der Azure AD-Mandant für Ihr Microsoft 365-Abonnement führt die Authentifizierung mit dem Cloudidentitätskonto durch.	Der Azure AD-Mandant für Ihr Microsoft 365-Abonnement behandelt verarbeitet entweder den Authentifizierungsprozess oder leitet den Benutzer an einen anderen Identitätsanbieter weiter.
Ideal für	Organisationen, die keinen lokalen AD DS besitzen oder benötigen.	Organisationen, die AD DS oder einen anderen Identitätsanbieter verwenden.
Größter Vorteil	Einfach zu verwenden. Es sind keine zusätzlichen Verzeichnistools oder Server erforderlich.	Benutzer können dieselben Anmeldeinformationen verwenden, wenn sie auf lokale oder cloudbasierte Ressourcen zugreifen.

Bei der ***reinen Cloudidentität*** werden Benutzerkonten verwendet, die nur in Azure AD vorhanden sind. Cloudidentitäten werden in der Regel von kleinen Organisationen verwendet, die keine lokalen Server haben oder AD DS nicht zum Verwalten lokaler Identitäten verwenden.

Nachfolgend die grundlegenden Komponenten der reinen Cloudidentität:

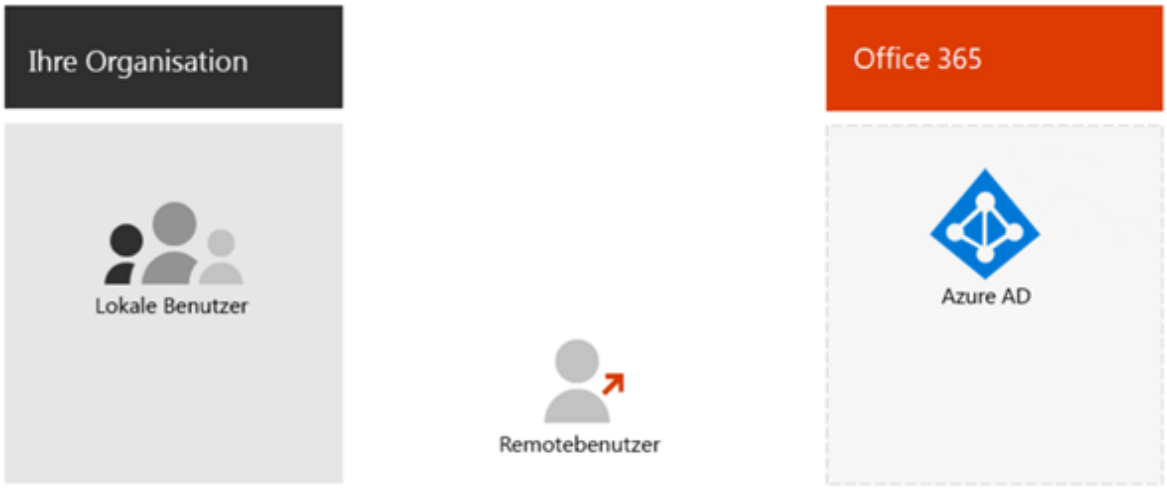


Abbildung 1: Reine Cloudidentität

Sowohl lokale als auch Remotebenutzer (Onlinebenutzer) verwenden Ihre Azure AD-Benutzerkonten und Kennwörter für den Zugriff auf Office 365-Clouddienste. Azure AD authentifiziert Benutzeranmeldeinformationen basierend auf den gespeicherten Benutzerkonten und Kennwörtern.

Da Benutzerkonten nur in Azure AD gespeichert sind, verwalten Sie Cloudidentitäten mit Tools wie dem Microsoft 365 Admin Center und Windows PowerShell mit dem Azure Active Directory PowerShell for Graph-Modul.

Die Hybrididentität verwendet Konten, die von einem lokalen AD DS stammen und eine Kopie im Azure AD-Mandanten eines Microsoft 365-Abonnements aufweisen. Die meisten Änderungen fließen jedoch nur in eine Richtung. Änderungen, die Sie an AD DS-Benutzerkonten vornehmen, werden mit Ihrer Kopie in Azure AD synchronisiert. Änderungen, die in cloudbasierten Konten in Azure AD vorgenommen wurden, wie zum Beispiel neue Benutzerkonten, werden jedoch nicht mit AD DS synchronisiert.

Azure AD Connect bietet die laufende Kontosynchronisierung. Es wird auf einem lokalen Server ausgeführt, überprüft auf Änderungen in AD DS und leitet diese Änderungen an Azure AD weiter. Azure AD Connect bietet die Möglichkeit zu filtern, welche Konten synchronisiert werden, und ob eine Hashversion der Benutzerkennwörter synchronisiert werden soll; dies wird als „Kennwort-Hash-Synchronisierung" (Password Hash Synchronization, PHS) bezeichnet.

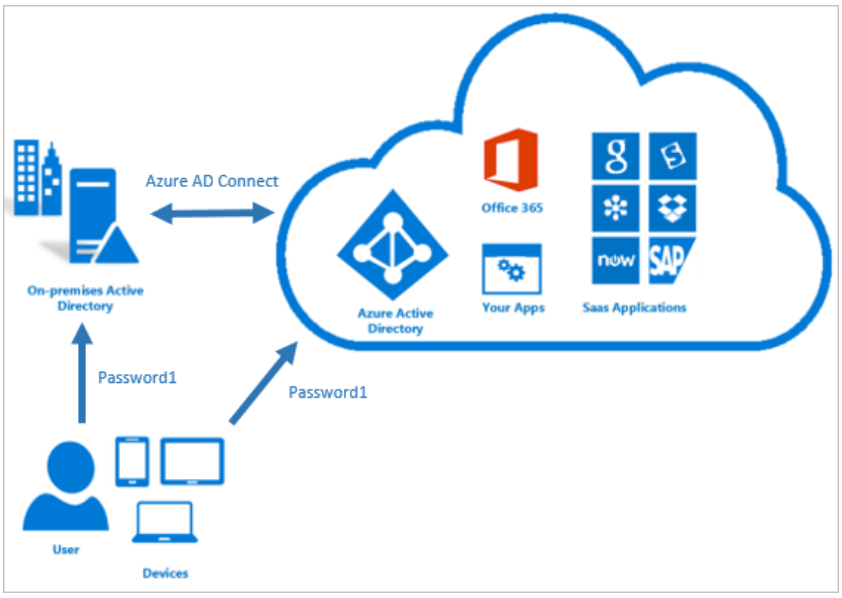


Abbildung 2: Password Hash Synchronization (PHS)

Wenn Sie die Hybrididentität implementieren, ist Ihr lokales AD DS die autorisierende Quelle für Kontoinformationen. Dies bedeutet, dass Sie Verwaltungsaufgaben hauptsächlich lokal durchführen, die dann mit Azure AD synchronisiert werden.

Nachfolgend finden Sie die Komponenten der Hybrididentität:

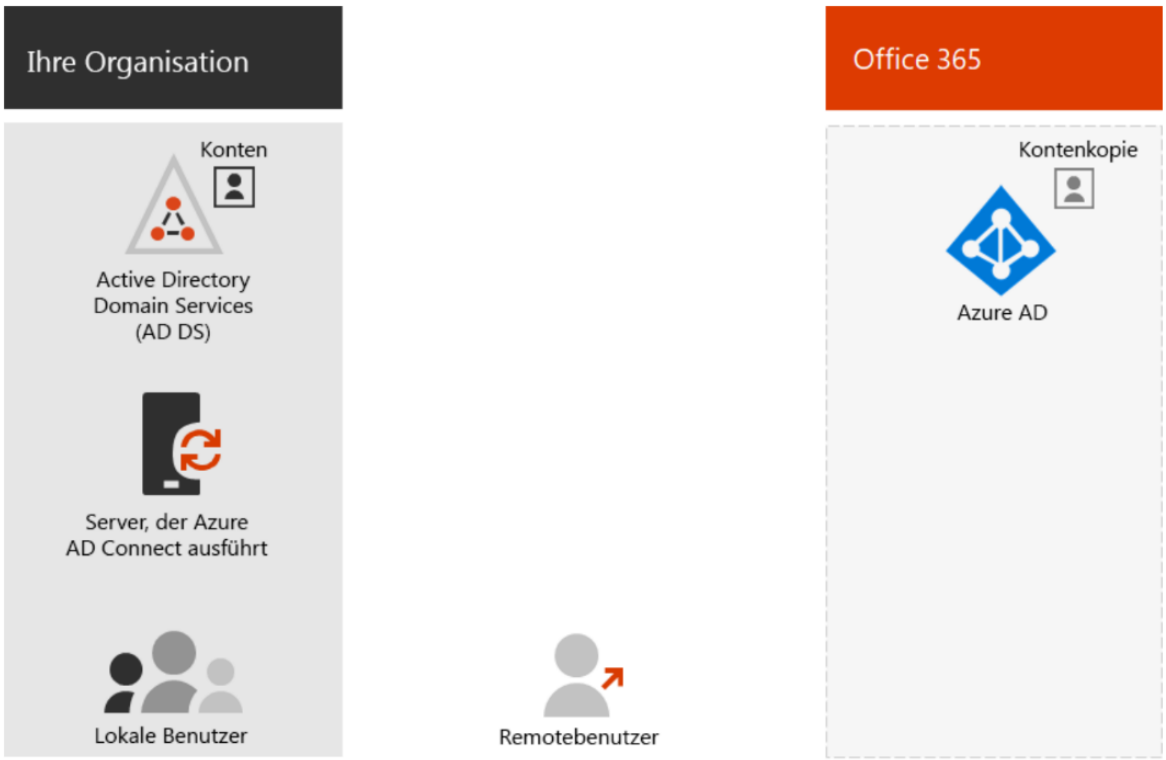


Abbildung 3: Hybride Identität

Der Azure AD-Mandant hat eine Kopie der AD DS-Konten. In dieser Konfiguration authentifizieren sich sowohl lokale als auch Remotebenutzer beim Zugriff auf Microsoft 365-Clouddienste bei Azure AD.

Da die ursprünglichen und autorisierenden Benutzerkonten im lokalen AD DS gespeichert sind, verwalten Sie Ihre Identitäten mit den gleichen Tools wie AD DS, zum Beispiel mit dem Tool „Active Directory-Benutzer und -Computer".

Sie verwenden nicht das Microsoft 365 Admin Center oder Windows PowerShell zum Verwalten von synchronisierten Benutzerkonten in Azure AD.

Mehr erfahren Sie hier: https://docs.microsoft.com/de-de/office365/enterprise/about-office-365-identity

Dokumentbeginn

Vorbereiten von Benutzern auf die Bereitstellung in Office 365 über die Verzeichnissynchronisierung

Wenn Sie über ein vorhandenes lokales Verzeichnis wie Active Directory verfügen, können Sie es in Azure AD integrieren, indem Sie Ihre Identitäten mit einem Synchronisierungstool wie Azure AD Connect aus dem lokalen Verzeichnis mit Microsoft 365 synchronisieren. In diesem Modell verwenden Sie weiterhin Ihre lokalen Verwaltungstools, um die Identitäten im lokalen Verzeichnis zu verwalten. Anschließend werden neue Konten und Änderungen automatisch mit Azure AD und damit mit Microsoft 365 synchronisiert.

Azure AD bietet Authentifizierung und Autorisierung für Microsoft 365 (einschließlich Microsoft Intune) und für andere Microsoft Cloud-Angebote, einschließlich Azure. Azure AD kann nur Cloudidentitäten oder Identitäten authentifizieren, die mit einem lokalen Verzeichnis synchronisiert sind, mit optionaler Kennwortsynchronisierung, oder Sie können die Benutzerauthentifizierung mit lokalen Benutzerkonten über Active Directory Federation Services (AD FS) oder eine andere einmalige Anmeldung aktivieren (SSO-Anbieter).

Für die Anbindung eines lokalen Active Directory empfiehlt sich für die Inbetriebnahme von Microsoft Teams die einfachste Methode über ***Password Hash Synchronisation (PHS)***. Die weiteren Methoden wie Pass Through Authentication (PTA) und ADFS-Verbundstruktur werden in diesem Guide bewusst aufgrund ihrer Komplexität nicht in Betracht gezogen.

Mehr erfahren Sie hier:

- https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization
- https://docs.microsoft.com/de-de/azure/active-directory/hybrid/how-to-connect-pta-how-it-works
- https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/how-to-connect-fed-azure-adfs

Password Hash Synchronisation (PHS) mit Single Sign-on

Dies ist die einfachste Möglichkeit, die Authentifizierung für lokale Verzeichnisobjekte in Azure AD zu aktivieren. Mit der Kennwort-Hash-Synchronisierung (PHS) synchronisieren Sie Ihre lokalen Active Directory-Benutzerkontoobjekte mit Microsoft 365 und verwalten Ihre Benutzer lokal. Hashes von Benutzerkennwörtern werden von Ihrem lokalen Active Directory mit Azure AD synchronisiert, sodass die Benutzer lokal und in der Cloud über dasselbe Kennwort verfügen. Wenn Kennwörter lokal geändert oder zurückgesetzt werden, werden die neuen Kennwort-Hashes mit Azure AD synchronisiert, sodass Ihre Benutzer immer dasselbe Kennwort für Cloudressourcen und lokale Ressourcen verwenden können. Die Kennwörter werden niemals an Azure AD gesendet oder im Klartext in Azure AD gespeichert.

Für einige Premiumfunktionen von Azure AD, zum Beispiel Identitätsschutz, ist PHS erforderlich, unabhängig davon, welche Authentifizierungsmethode ausgewählt ist. Mit der nahtlosen einmaligen Anmeldung werden Benutzer automatisch bei Azure AD angemeldet,

wenn sie sich auf ihren Unternehmensgeräten befinden und mit Ihrem Unternehmensnetzwerk verbunden sind.

In Microsoft 365 wird die Verzeichnissynchronisierung häufig zum Synchronisieren in eine Richtung verwendet (von lokal zu Azure AD). Einige Funktionen in ***Azure AD Connect*** ermöglichen jedoch das Zurückschreiben bestimmter Objekte und Attribute in das lokale Verzeichnis. Erstellen Sie daher eine Art bidirektionale Synchronisation. Zusätzlich zu Verzeichnisobjekten kann die Verzeichnissynchronisierung auch die bidirektionale Synchronisierung von Benutzerkennwörtern ermöglichen. Verzeichnissynchronisierungstools, die diese Synchronisierung durchführen, zum Beispiel Azure AD Connect, sollten auf einem dedizierten Computer in Ihrer lokalen Umgebung installiert werden.

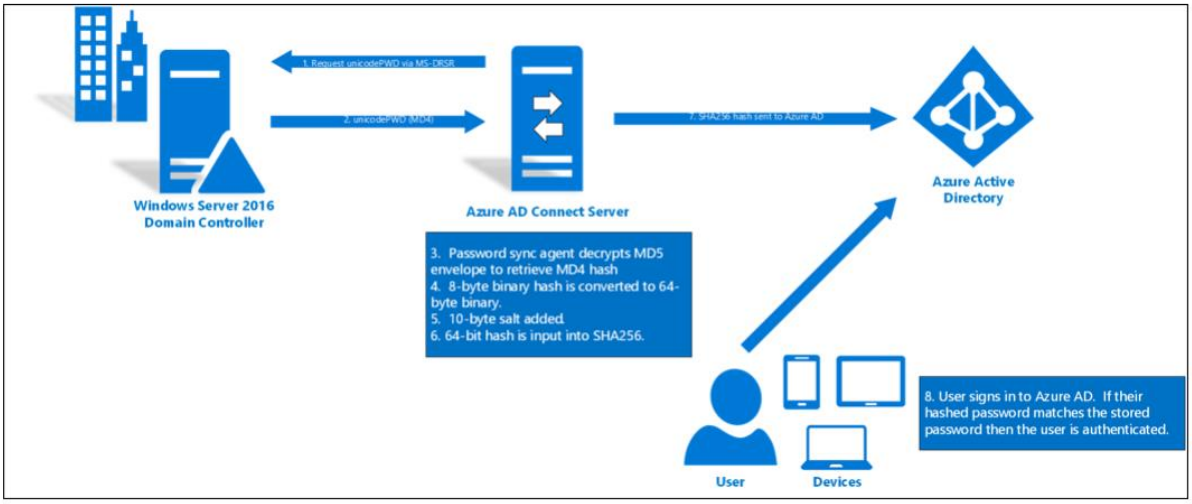


Abbildung 4: Single Sign-on mit Azure AD

Das Azure Active Directory Connect-Tool (***Azure AD Connect***) ist das offiziell empfohlene Verzeichnissynchronisierungstool für Microsoft 365. Azure AD Connect ist als von Ihnen konfiguriertes softwarebasiertes Tool konzipiert, und es wird automatisch im Hintergrund ohne Benutzerinteraktion ausgeführt. Für Microsoft 365 besteht der Zweck des Tools darin, die Koexistenz zwischen Ihrer lokalen Active Directory-Umgebung und Microsoft 365 in der Cloud zu ermöglichen.

Azure AD Connect besteht aus drei Teilen: den Synchronisierungsdiensten, dem optionalen Teil der Active Directory-Verbunddienste und dem Überwachungsteil, der mit Azure AD Connect Health ausgeführt wird.

Bevor Sie die Verzeichnissynchronisierung bereitstellen, um Ihre lokalen Active Directory-Objekte mit Azure AD zu synchronisieren, müssen Sie Ihre Umgebung vorbereiten, indem Sie die folgenden Funktionen analysieren:

- Active Directory-Vorbereitung
- UPN-Suffixe
- Microsoft 365-Bereitschaftsprüfungen
- Microsoft 365 IdFix-Tool

Nachdem Sie die Verzeichnissynchronisierung aktiviert haben, können Sie synchronisierte Objekte nur mit Ihren lokalen Active Directory-Verwaltungstools bearbeiten.

Bei der Vorbereitung der Bereitstellung der Verzeichnissynchronisierung sollte Ihr Projektplan die Active Directory-Vorbereitung sowie die Anforderungen und Funktionen von Azure AD enthalten. So bereiten Sie Active Directory vor:

- Identifizieren Sie die Quelle der Autorität.
- Bereinigen Sie Active Directory.
- Richten Sie Auditing ein.

Obwohl Azure AD Connect einfach zu implementieren ist, müssen Sie die Implementierung des Azure AD Connect-Tools gründlich planen, wenn Sie eine komplexe Active Directory-Implementierung oder spezielle Anforderungen (zum Beispiel teilweise Attributsynchronisierung) haben. Um mit Ihrer Planung zu beginnen, sollten Sie Antworten auf die folgenden Fragen sammeln:

- Auf welchem Server möchten Sie Azure AD Connect installieren?
- Benötigen Sie ein Azure AD Connect-Failover-Szenario?
- Möchten Sie ein oder mehrere Active Directorys (oder mehrere Forests) synchronisieren?
- Möchten Sie Ihr Active Directory ganz oder nur teilweise synchronisieren? Möchten Sie alle Objektattribute synchronisieren oder bestimmte Filter verwenden?
- Möchten Sie erweiterte Konfigurationsfunktionen wie Kennwortsynchronisierung, Kennwortrückschreibung oder Geräterückschreibung verwenden?

Ihre Entscheidung, ob Sie die Kennwort-Hash-Synchronisierung implementieren möchten, wirkt sich auf Ihre nächsten Schritte aus. Beachten Sie Folgendes in Bezug auf die Synchronisierung von Kennwort-Hashs:

Wenn Sie die Kennwort-Hash-Synchronisierung implementieren, kann sich der Benutzer mit demselben Benutzernamen und Kennwort wie im lokalen AD authentifizieren. Azure AD Connect synchronisiert Ihren Kennwort-Hash (einen kryptografischen Hash des Kennwort-Hash) und speichert ihn im jeweiligen Benutzerobjekt in Azure AD.

Vor der Installation von Azure AD Connect müssen Sie die folgenden Themen berücksichtigen, um zu entscheiden, auf welchem Server das Tool installiert werden soll:

- Kann auf einem Domänencontroller, Mitgliedsserver oder einem Server ohne Domänenbeitritt installiert werden.
- Unterstützt Windows Server 2008 oder höher.
- Wenn Ihr Active Directory weniger als 100.000 Objekte enthält, können Sie die Light-Version von SQL Server Express verwenden, die auf dem Azure AD Connect-Server installiert wird.
- Wenn Sie mehr als 100.000 Objekte haben, müssen Sie einen zusätzlichen SQL Server planen, um die Datenbank zu verwalten und zu laden.

Es kann nicht mehr als ein Azure AD Connect-Server mit einem einzelnen Azure AD- oder Microsoft 365-Mandanten verbunden sein. Zwischen einem Azure AD-Mandanten und einem Server, auf dem Azure AD Connect ausgeführt wird, besteht ein Verhältnis von 1: 1. Wenn Sie mehr als einen Azure AD Connect-Server haben möchten, müssen Sie mehr als einen Azure AD-Mandanten bereitstellen.

In der folgenden Tabelle sind die Mindesthardwareanforderungen für den Azure AD Connect-Synchronisierungscomputer aufgeführt.

Tabelle 3: Hardwareanforderungen für Azure AD Connect

Number of objects in AD	CPU	RAM	Hard drive size
< 10,000	1.6 GHz	4 GB	70 GB
10,000-50,000	1.6 GHz	4 GB	70 GB
50,000-100,000	1.6 GHz	16 GB	100 GB
100,000-300,000	1.6 GHz	32 GB	300 GB
300,000-600,000	1.6 GHz	32 GB	450 GB
> 600,000	1.6 GHz	32 GB	500 GB

Azure AD Connect unterstützt die Installation zusätzlicher Server im Staging-Modus. Ein Server in diesem Modus liest Daten aus allen verbundenen Verzeichnissen, schreibt jedoch nichts in verbundene Verzeichnisse. Es verwendet den normalen Synchronisationszyklus und verfügt daher über eine aktualisierte Kopie der Identitätsdaten.

Wenn der Primärserver ausfällt, können Sie im Azure AD Connect-Assistenten ein Failover auf den Staging-Server durchführen. Dieser zweite Server kann sich in einem anderen Rechenzentrum befinden, in dem keine Infrastruktur für den Primärserver freigegeben ist. Sie müssen alle auf dem Primärserver vorgenommenen Konfigurationsänderungen manuell auf den zweiten Server kopieren.

Ein weiterer wichtiger Planungsaspekt für Azure AD Connect ist die Entscheidung, welches Objekt als sourceAnchor verwendet werden soll. Das sourceAnchor-Attribut stimmt sowohl mit dem Quell- als auch mit dem Zielobjekt überein, wodurch beide Objekte miteinander verknüpft werden. Aus diesem Grund identifiziert sourceAnchor ein Objekt sowohl in Ihrem lokalen Active Directory als auch in Azure AD eindeutig als dasselbe Objekt. Der sourceAnchor sollte ein Objekt sein, das sich niemals ändern wird.

Mehr erfahren Sie hier: Azure AD Connect-Synchronisierung: Mit Azure Active Directory synchronisierte Attribute

Wenn Sie Azure AD Connect mit Express-Einstellungen installieren, muss der Verzeichnissynchronisierungscomputer Mitglied einer Domäne sein. In Szenarien mit einer einzelnen Gesamtstruktur muss dieser Computer einer Domäne innerhalb derselben Gesamtstruktur zugeordnet sein, die synchronisiert wird.

Auf der anderen Seite können Sie mit benutzerdefinierten Einstellungen Azure AD Connect auf einem Computer installieren, der keiner Domäne angehört. Azure AD Connect unterstützt auch die Installation auf Domänencontrollern. In den meisten Szenarien wird jedoch empfohlen, einen Mitgliedsserver für Azure AD Connect zu verwenden.

Für Azure AD Connect sind die folgenden Windows Server-Versionen erforderlich (nur 64-Bit-Edition):

- Windows Server 2008 oder 2008 R2
- Windows Server 2012, 2012 R2
- Windows Server 2016

Wenn Sie die Funktion zur Kennwortsynchronisierung oder zum Zurückschreiben von Kennwörtern verwenden möchten, muss sich der Server unter Windows Server 2008 R2 oder höher befinden.

Das zum Installieren und Konfigurieren von Azure AD Connect verwendete Konto muss über die folgenden Berechtigungen verfügen:

- Ein globales Administratorkonto, das Mitglied der globalen Administratorrolle in Ihrem Microsoft 365-Mandanten ist.
- Ein Enterprise Administrator-Konto für Ihr lokales Active Directory. Dies ist erforderlich, um das Verzeichnissynchronisierungsdienstkonto in Active Directory zu erstellen.
- Lokale Administratorberechtigung auf dem Azure AD Connect-Computer. Dies ist erforderlich, um das Azure AD Connect-Tool zu installieren.

Während der Installation von Azure AD Connect können Sie die Express-Einstellungen auswählen. Dies ist die Standardoption und eines der häufigsten Installationsszenarien. Beim Ausführen des Express-Setups stellt Azure AD Connect die Synchronisierung mit der Option zur Kennwortsynchronisierung bereit. Dies gilt nur für eine einzelne Gesamtstruktur und ermöglicht Ihren Benutzern, sich mit ihrem lokalen Kennwort bei Microsoft 365 anzumelden.

Express-Einstellungen sollten verwendet werden, wenn eines der folgenden Szenarien vorliegt:

- Sie haben eine einzelne Active Directory-Gesamtstruktur.
- Benutzer melden sich mit demselben Kennwort mithilfe der Kennwort-Hash-Synchronisierung an.

Während der Installation von Azure AD Connect mit Express-Einstellungen führt das Installationsprogramm Folgendes aus:

1. Installieren der Synchronisations-Engine
2. Konfigurieren von Azure AD Connect

3. Konfigurieren des lokalen Active Directory-Connectors
4. Aktivieren der Kennwort-Hash-Synchronisierung
5. Konfigurieren von Synchronisierungsdiensten
6. Konfigurieren von Synchronisierungsdiensten für die Exchange-Hybridbereitstellung (optional)
7. Aktivieren von automatischen Upgrades von Azure AD Connect

Wenn Sie die Express-Einstellungen verwenden, wird die Synchronisierung nach Abschluss der Installation automatisch gestartet (Sie können dies jedoch auch nicht tun).

Mehr erfahren Sie hier: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express

Mit Azure AD Connect Health können Sie Ihre lokale Identitätsinfrastruktur und die über Azure AD Connect verfügbaren Synchronisierungsdienste überwachen und Einblicke in diese gewinnen. Es bietet Ihnen die Möglichkeit, Warnungen, Leistung, Verwendungsmuster und Konfigurationseinstellungen anzuzeigen und eine zuverlässige Verbindung zu Microsoft 365 aufrechtzuerhalten. Dies wird mithilfe eines Agenten erreicht, der auf den Zielservern installiert ist.

Mehr erfahren Sie hier: https://docs.microsoft.com/de-de/azure/active-directory/hybrid/whatis-hybrid-identity

Es sind mehrere Verwaltungsaufgaben erforderlich, die Sie als Sicherheits- und Compliance-Administrator ausführen müssen, um sicherzustellen, dass Benutzer effizient synchronisiert werden und Azure AD Connect erfolgreich bereitgestellt wird. Diese Aufgaben umfassen:

- Verwaltung von Benutzerkonten
- Wiederherstellung eines Benutzerkontos, das versehentlich gelöscht wurde
- Wiederherstellung nach nicht synchronisierten Löschvorgängen
- Verbesserte Benutzerverwaltung

Es ist wichtig zu beachten, dass Sie Benutzerobjekte mit Ihrem lokalen Active Directory-Snap-in für Benutzer und Computer oder Windows PowerShell in Ihrem lokalen Active Directory erstellen, ändern und löschen. Sie können synchronisierte Benutzerkonten nicht mit dem Microsoft 365 Admin Center oder dem Exchange Online Admin Center (EAC) verwalten, da nicht alle synchronisierten Attribute wieder mit Ihrer lokalen Umgebung synchronisiert werden. Im Microsoft 365 Admin Center müssen nur einige zusätzliche Attribute verwaltet werden, die in Ihrem Active Directory nicht verfügbar sind, zum Beispiel:

- Microsoft 365-Produktlizenzen
- Erweiterte Exchange Online-Einstellungen, zum Beispiel Aktivieren der direkten Archivierung

Azure AD unterstützt weiche Löschvorgänge. Diese Funktion ist auch verfügbar, wenn Sie Benutzer in Ihrem lokalen Active Directory löschen und das Löschen mit Microsoft 365 synchronisiert wird. In diesem Fall wird das Benutzerobjekt in einen gelöschten Zustand

versetzt und nicht mehr in der Benutzerliste angezeigt, und die Lizenz kann neu zugewiesen werden. Das Benutzerobjekt wird nur dann mit einem lokalen Objekt verknüpft, wenn Sie es wiederherstellen oder ein neues Objekt mit demselben Quellanker erstellen. Das Benutzerobjekt kann jedoch innerhalb von 30 Tagen für eine Organisation wiederhergestellt werden. Sie können entweder das Microsoft 365 Admin Center oder Windows PowerShell verwenden, um gelöschte Benutzerobjekte wiederherzustellen:

1. Klicken Sie im Microsoft 365 Admin Center im linken Navigationsbereich im Menü „Benutzer" auf „Gelöschte Benutzer".
2. Wählen Sie das gelöschte Benutzerkonto aus, das Sie wiederherstellen möchten, und klicken Sie dann auf „Wiederherstellen".
3. Wählen Sie auf der Seite „Wiederherstellen" entweder „Kennwort automatisch generieren" oder „Kennwort erstellen" lassen. Wenn Sie die Kennwortsynchronisierung aktiviert haben, wird die Auswahl beim nächsten Kennwortsynchronisierungszyklus überschrieben.
4. Wenn Sie Windows PowerShell bevorzugen, können Sie das Cmdlet Restore-MsolUser verwenden, um ein Benutzerobjekt wiederherzustellen.

Wenn Sie versehentlich ein Benutzerkonto löschen und ein Verzeichnissynchronisierungszyklus ausgeführt wird, wird das Benutzerkonto in Microsoft 365 gelöscht. Wenn Sie jedoch die Papierkorbfunktion in Active Directory aktiviert haben, können Sie das Konto aus dem Papierkorb wiederherstellen und der Link zwischen den Konten wird wiederhergestellt. Wenn Sie den Papierkorb nicht aktiviert haben, müssen Sie möglicherweise ein anderes Konto mit einer neuen GUID erstellen.

Mehr erfahren Sie hier: https://support.microsoft.com/en-us/help/2619308/how-to-troubleshoot-deleted-user-accounts-in-office-365-azure-and-intu

Eine weitere wichtige Wartungsaufgabe ist das Löschen vor Ort, das nicht mit Microsoft 365 synchronisiert wird. In diesem Fall wird das verknüpfte Objekt nicht aus Azure AD entfernt. Diese Situation kann auftreten, wenn die Verzeichnissynchronisierung noch nicht abgeschlossen ist oder wenn bei der Verzeichnissynchronisierung ein bestimmtes Cloudobjekt nicht gelöscht werden konnte. Beides führt zu einem verwaisten Azure AD-Objekt.

Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

1. Führen Sie manuell ein Verzeichnissynchronisierungsupdate aus. Sie können entweder den Synchronization Service Manager von Azure AD Connect oder Windows PowerShell mit dem Cmdlet Start-ADSyncSyncCycle -PolicyType Delta archivieren, um dies zu archivieren.
2. Überprüfen Sie, ob die Verzeichnissynchronisierung korrekt durchgeführt wurde. Öffnen Sie den Synchronization Service Manager und überprüfen Sie, ob alle Synchronisierungen abgeschlossen sind. In der Statuszeile wird „Erfolgreich" angezeigt.
3. Überprüfen Sie die Verzeichnissynchronisierung. Öffnen Sie das Microsoft 365 Admin Center und überprüfen Sie, ob die Objekte wie erwartet gelöscht wurden.
4. Entfernen Sie gegebenenfalls verwaiste Objekte.

Wenn Sie diese Schritte ausführen und überprüfen, ob die Verzeichnissynchronisierung ordnungsgemäß funktioniert, das Löschen des Active Directory-Objekts jedoch noch nicht an Azure AD weitergegeben wurde, kann das verwaiste Objekt mithilfe eines der folgenden Windows PowerShell-Cmdlets manuell entfernt werden:

- Remove-MsolUser
- Remove-MsolContact
- Remove-MsolGroup

Führen Sie beispielsweise das folgende Cmdlet aus, um einen verwaisten Benutzer mit dem UPN StellaC@adatum.com, der ursprünglich mithilfe der Verzeichnissynchronisierung erstellt wurde, manuell zu entfernen:

Remove-MsolUser –UserPrincipalName [StellaC@adatum.com] (mailto: StellaC@adatum.com)

Azure AD Connect bietet zusätzliche erweiterte Benutzerverwaltungsfunktionen, einschließlich Zurückschreiben von Kennwörtern und Zurückschreiben von Geräten.

Benutzer können ihre Kennwörter über die Anmeldeseite oder über Benutzereinstellungen in Microsoft 365 ändern und sie in das lokale Active Directory des Unternehmens zurückschreiben lassen. Um diese Funktion zu aktivieren, benötigen Sie Folgendes:

Windows Server 2008 oder höhere Domänencontroller in Ihrem lokalen Active Directory. Für Windows 2008- oder Windows 2008 R2-Domänencontroller muss außerdem KB2386717 installiert sein.

Konfiguration der SSPR-Option (Self-Service Password Reset) in Ihrem Office 365-Mandanten

Um die Kennwortrückschreibungsfunktion für Azure AD Connect zu aktivieren, müssen Sie die entsprechende Option während der Installation von Azure AD Connect aktivieren. Dazu müssen Sie die Option „Benutzerdefiniertes Setup“ auswählen, wenn Sie den Azure AD Connect-Installationsassistenten ausführen. Sobald Sie Ihr Azure AD-Setup abgeschlossen haben, wird Folgendes konfiguriert:

- Die Azure AD Connect-Connectors, die zum Zurücksetzen des Kennworts aktiviert sind.
- Das Azure AD Connect-Dienstkonto für lokales Active Directory, das die Berechtigung zum Zurücksetzen von Kennwörtern für Objekte in Ihrer Organisationseinheit benötigt.

Sie können die Berechtigungen für Active Directory-Benutzer und -Computer für diese Organisationseinheit anzeigen, wenn Sie den erweiterten Modus aktivieren. Das Kontrollkästchen für die Berechtigungseingabe muss für die folgenden Berechtigungen aktiviert sein:

- Passwort ändern
- Passwort zurücksetzen
- Schreibberechtigung für die Eigenschaft lockoutTime

- Schreibberechtigung für pwdLastSet-Eigenschaft

Sie können die Funktion zum Zurückschreiben von Kennwörtern testen, die mit dem Ändern Ihres Kennworts mithilfe des Self-Service-Kennwortrücksetzens in Ihrem Microsoft 365-Mandanten identisch ist.

Dokumentbeginn

Azure-basierte Multi-Faktor-Authentifizierung (MFA)

Bei der Nutzung von Clouddiensten wie Microsoft Teams helfen Ihre bisherigen Schutzmechanismen wie Perimetersysteme nur bedingt. Um den Zugriff auf Unternehmensdaten in der Cloud auf tatsächlich berechtigte Benutzer einzuschränken, bietet sich die Multi-Faktor-Authentifizierung an.

Grundsätzlich gibt es in der Microsoft 365-Welt zwei Möglichkeiten, MFA zu aktivieren:

1. Azure AD MFA, auch User-Based MFA genannt
2. Conditional Access MFA

Wenn Sie die Möglichkeiten (Lizenzen) haben, empfiehlt Microsoft die Verwendung von ***Conditional Access MFA***, um für zukünftige Szenarien nichts verbaut zu haben, weil Azure MFA bei jeder Anmeldung immer MFA verlangt, wohingegen bei Conditional Access auch weitere Bedingungen evaluiert werden. ***Wenn Sie dieser Empfehlung folgen wollen, überspringen Sie dieses Kapitel und gehen Sie direkt zum Kapitel Conditional Access.***

Azure AD MFA ist darauf ausgelegt, dem Administrator eine möglichst einfache und entlastende Konfiguration und gleichzeitig dem Benutzer die Freiheit der MFA-Methode zu ermöglichen. Damit verbunden muss jedoch jeder Nutzer für sich selbst die MFA-Methode aktivieren.

Um Azure AD MFA zu aktivieren, öffnen Sie das Azure Portal und folgen Sie der Navigation:

Azure Active Directory → Sicherheit → MFA → Erste Schritte

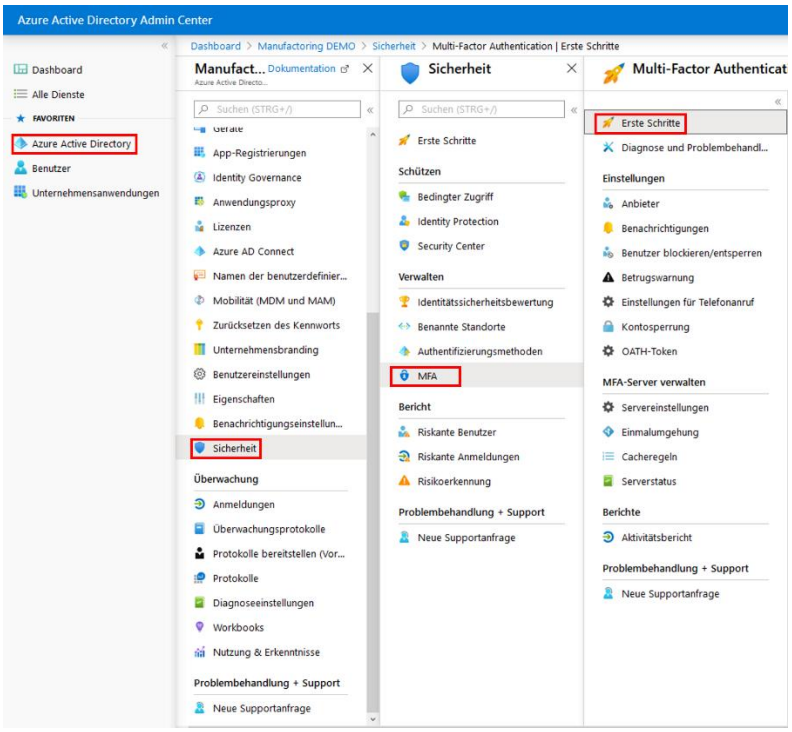


Abbildung 5: MFA-Konfiguration im Azure Portal

Klicken Sie auf der Seite „Erste Schritte“ in der Mitte auf den Link „Zusätzliche cloudbasierte MFA-Einstellungen“, um die Konfiguration in einem neuen Tab/Fenster zu öffnen.

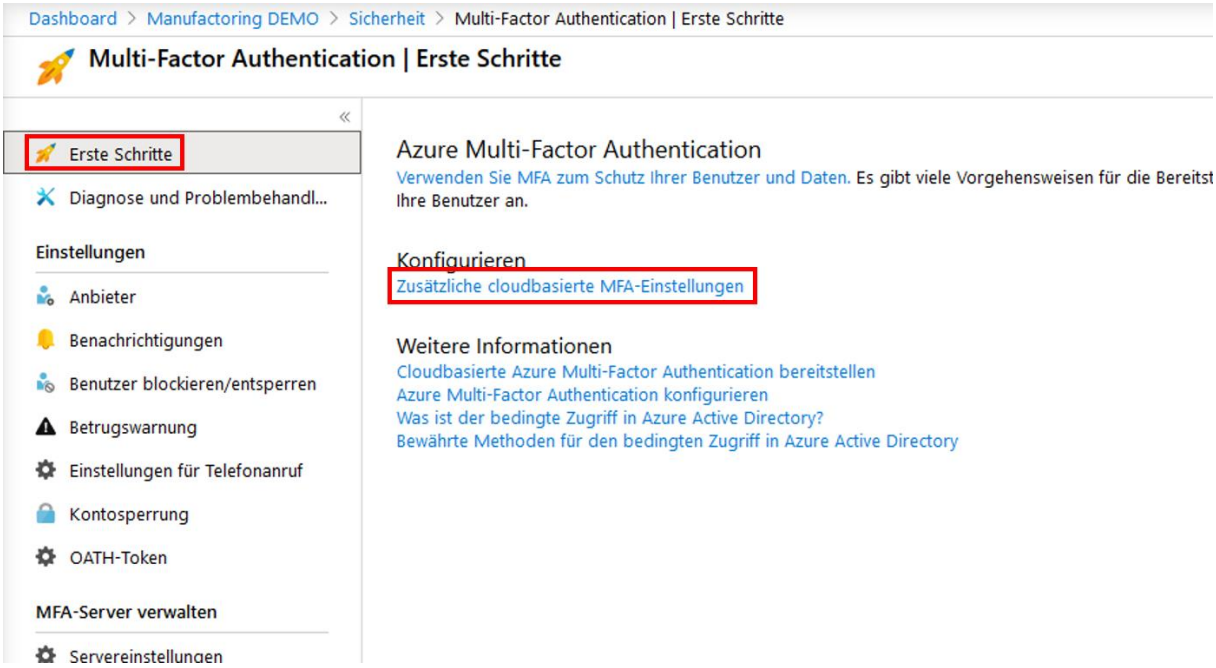


Abbildung 6: Erste Schritte der MFA Einstellungen

In den „Diensteinstellungen“ haben Sie nun vier Konfigurationsmöglichkeiten:

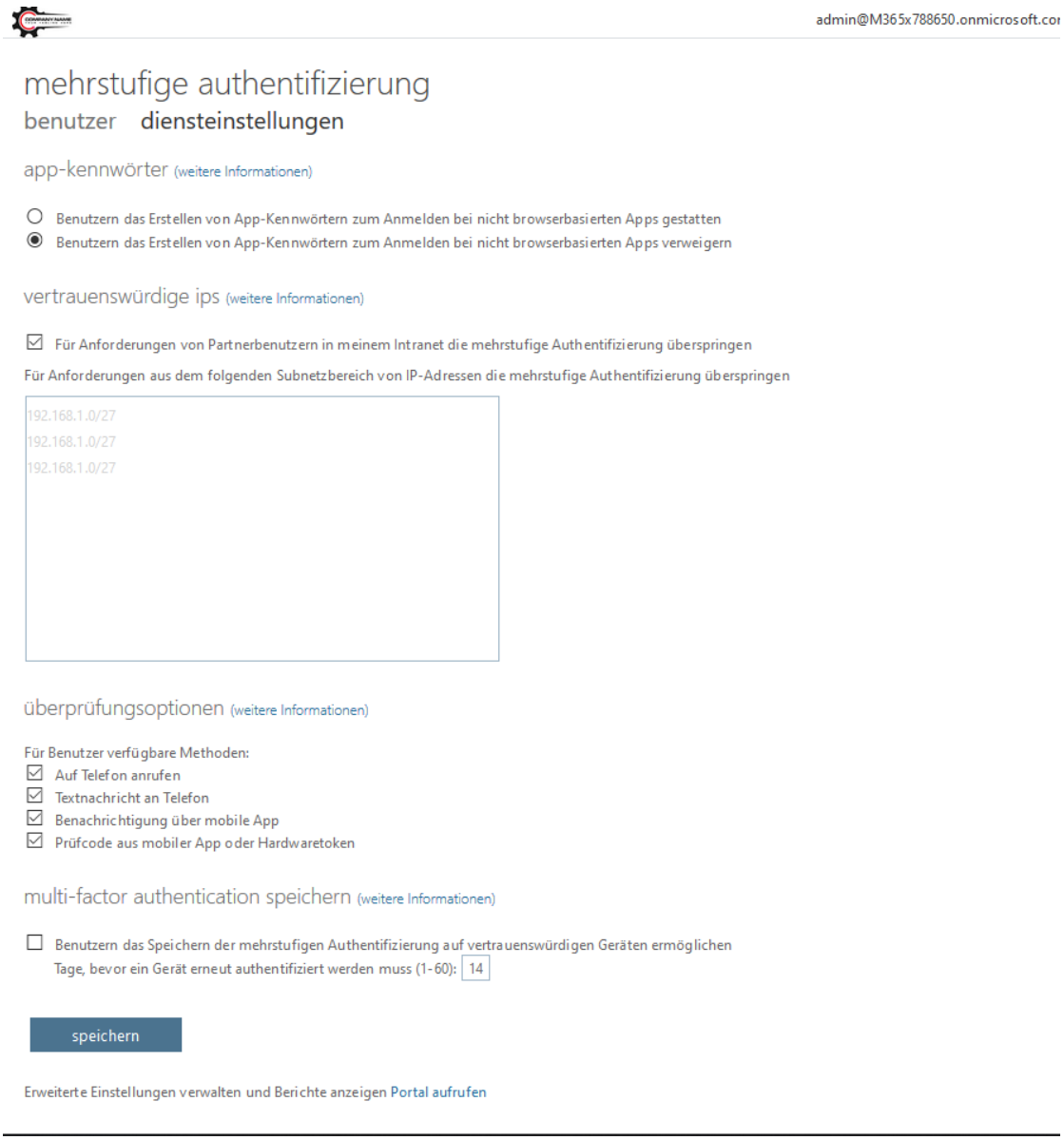
1. **App-Kennwörter**
   App-Kennwörter werden für Office 2010 und ältere Applikationen benötigt, weil diese keine modernen Authentifizierungsmethoden unterstützen und anstelle von MFA ein App-Kennwort verwendet wird. Mit App-Kennwörtern gehen jedoch mehrere Einschränkungen und Schwierigkeiten einher, deshalb ist die Empfehlung, die verwendeten Applikationen auf einen aktuellen Stand zu bringen und App-Kennwörter nicht zu verwenden.
   Weitere Informationen zu Bedingungen und Einschränkungen finden Sie hier: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#app-passwords
2. **Vertrauenswürdige IPs**
   An dieser Stelle können Sie IPv4-Adressen angeben, von denen sich Benutzer anmelden können, ohne eine Multi-Faktor-Authentifizierung durchführen zu müssen. Die unternehmenseigenen IP-Adressen bieten sich dafür an.
3. **Überprüfungsoptionen**
   Als Administrator können Sie angeben, welche Methoden Sie Ihren Benutzern zur Verfügung stellen. Bedenken Sie bei der Auswahl, welche Optionen dem Benutzer überhaupt zur Verfügung stehen. Nicht alle haben beispielsweise ein (Unternehmens-) Smartphone. Es gibt vier Auswahlmöglichkeiten:
   1. Auf Telefon anrufen: Hier gibt der Benutzer eine beliebige Telefonnummer an und erhält einen automatischen Anruf, den er mit einer vorher eingestellten PIN

bestätigen muss. Dieses Szenario ist auch für Produktionshallen gut geeignet, weil ein Telefon von mehreren Benutzern verwendet werden kann.

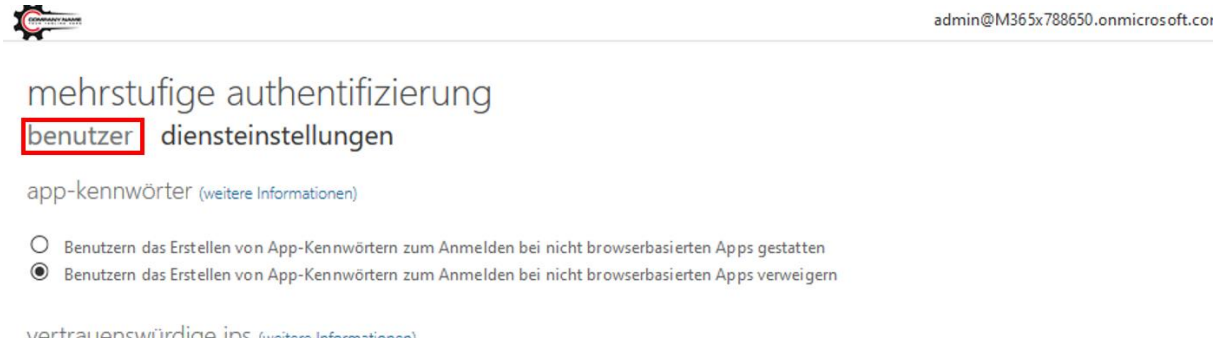
2. Textnachricht an Telefon: Der Benutzer erhält eine SMS mit einem Einmalcode. Wichtig: Das (Mobil-) Telefon muss SMS empfangen können.
3. Benachrichtigung über mobile App: Hierfür muss der Benutzer die „Authenticator App" aus dem App Store auf seinem Smartphone installiert haben. Beim Einrichten wird dem Benutzer ein QR-Code angezeigt, der mithilfe der App gescannt wird, um das Einrichten abzuschließen. Bei der Multi-Faktor-Authentifizierung erhält der Benutzer eine Push-Benachrichtigung und muss diese mit einer PIN oder Biometrie bestätigen.
4. Prüfcode aus mobiler App: Die Einrichtung erfolgt wie bei Option 3. Der Benutzer muss für MFA die App öffnen. Hierbei wird dem Benutzer ein 6-stelliger Prüfcode angezeigt, der sich alle 30 Sekunden ändert. Dieser Prüfcode muss im Anmeldefenster eingegeben werden.

4. MFA speichern

Mit dieser Funktion können Sie einstellen, dass die Benutzer nicht bei jeder Anmeldung eine MFA durchführen müssen. Für Browser-Anwendungen wird dies mit Cookies realisiert, für Nicht-Browser-Anwendungen mithilfe von (Refresh-)Tokens. Bedenken Sie: Mit jedem zusätzlichen Tag verringern Sie die Sicherheit Ihrer Anwendungen!

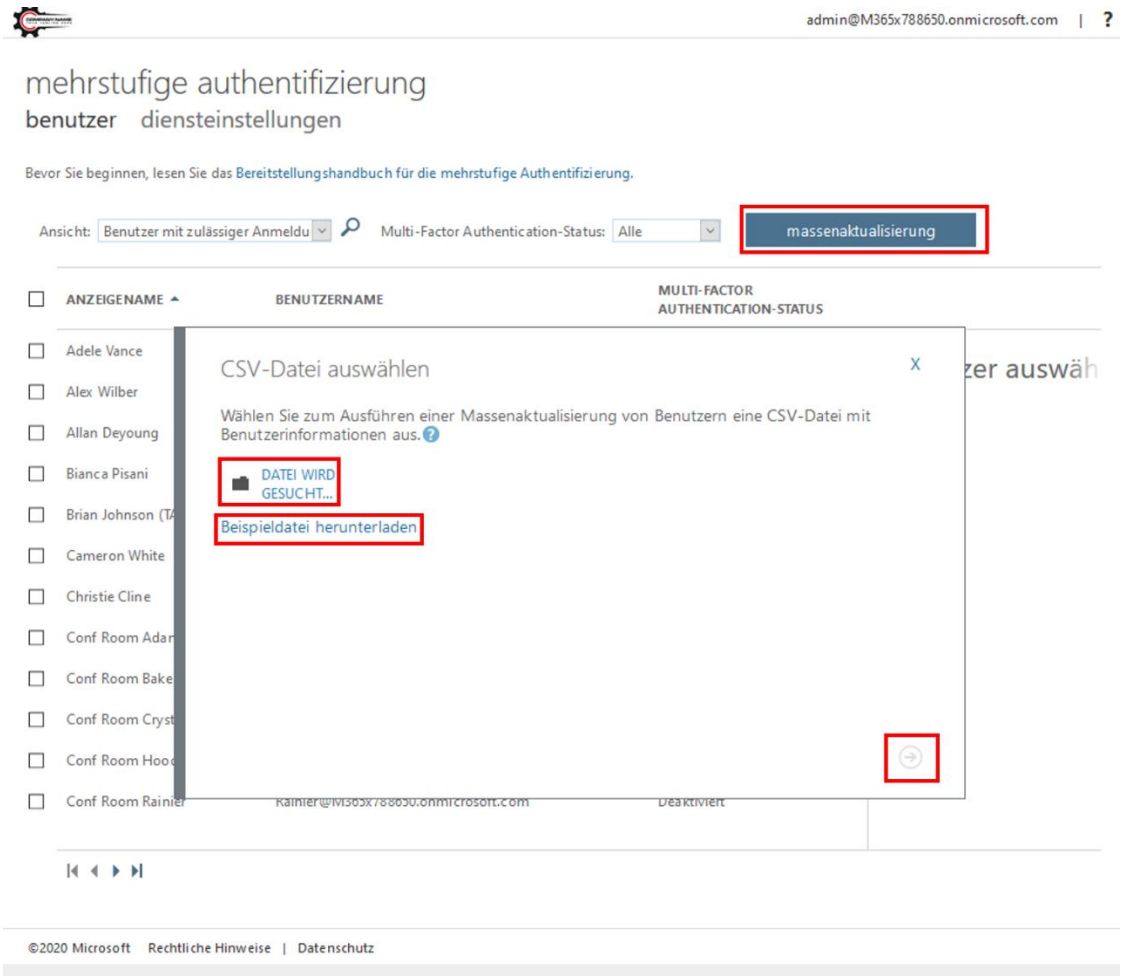


Zu guter Letzt müssen Sie MFA für die Benutzer aktivieren. Klicken Sie oben auf „Benutzer“.



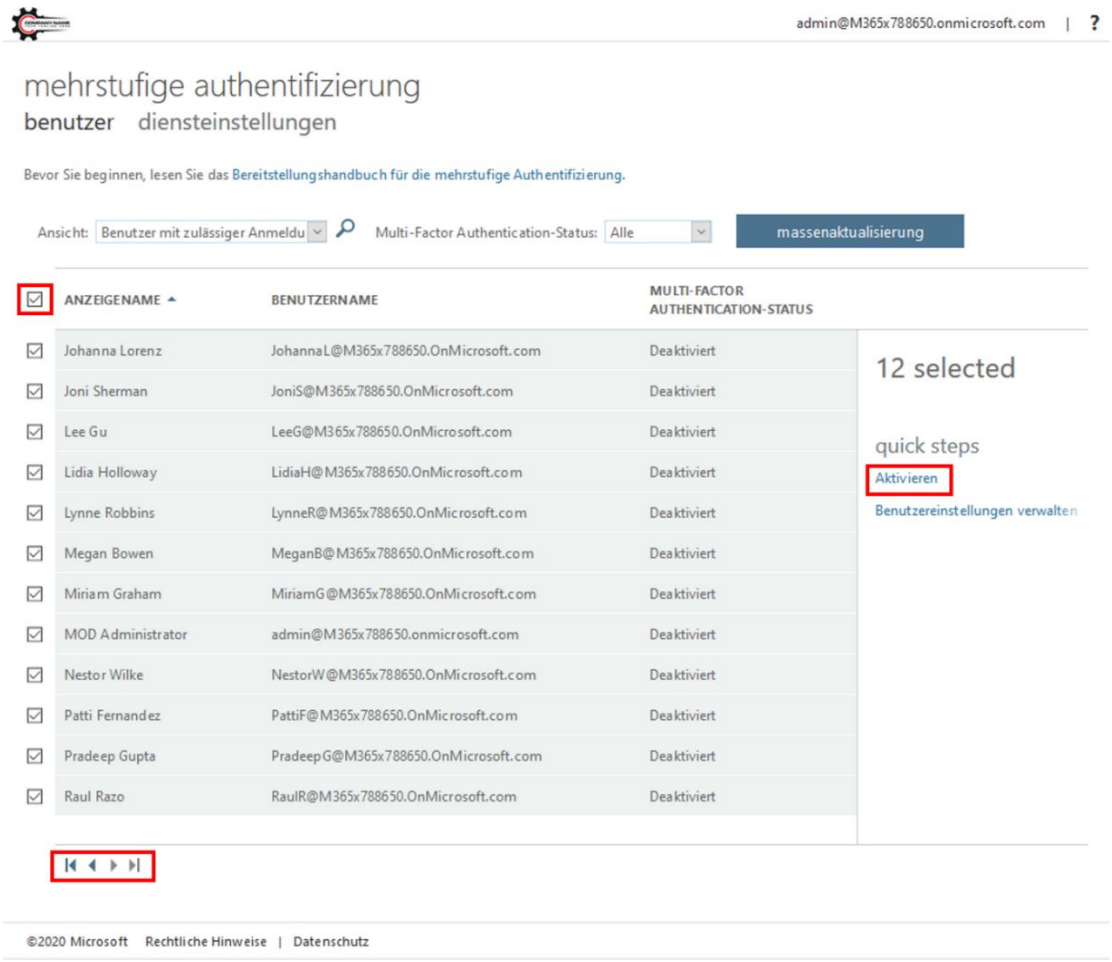
Um die Benutzer für MFA zu aktivieren, verwenden Sie eine der zwei Möglichkeiten:

1. Massenaktualisierung: Hierbei muss eine CSV-Datei mit allen Benutzern, exakt nach dem Schema der Beispieldatei, hochgeladen werden.



oder

2. Aktualisierung über die Benutzeroberfläche: Wählen Sie über die Checkbox alle Benutzer dieser Seite aus und klicken Sie im rechten Menü auf „Aktivieren“. Dies müssen Sie für jede Seite der Benutzer separat tun, was bei einer hohen Anzahl zeitaufwendig sein kann.



Dokumentbeginn

Conditional Access

Um Conditional Access (auf Deutsch: Bedingter Zugriff) zu aktivieren, öffnen Sie das Azure Portal und folgen Sie der Navigation: Azure Active Directory → Sicherheit → Bedingter Zugriff

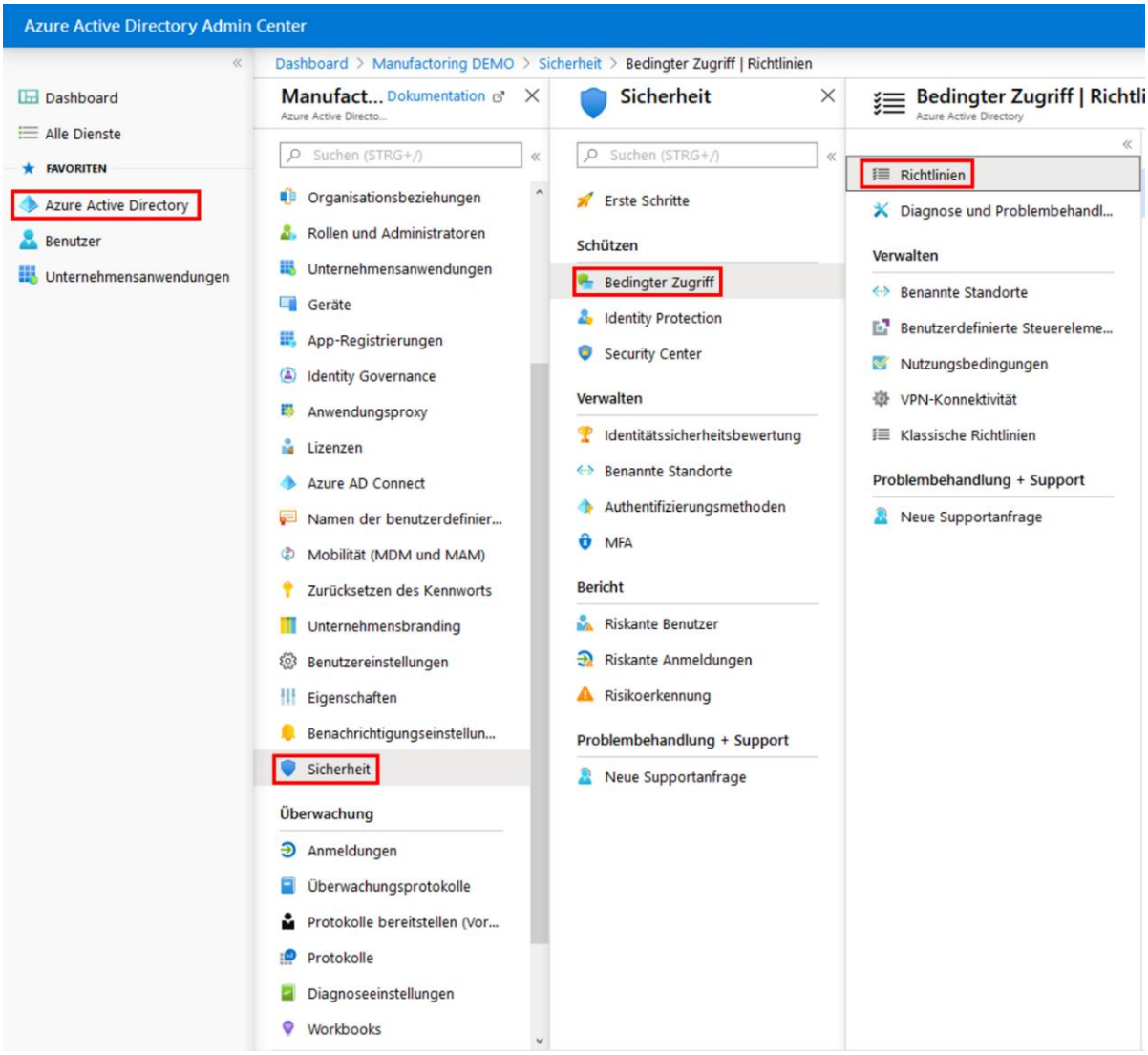


Abbildung 7: Bedingter Zugriff im Azure Portal

Um eine neue Richtlinie (Policy) zu erstellen, klicken Sie auf „+ Neue Richtlinie“.

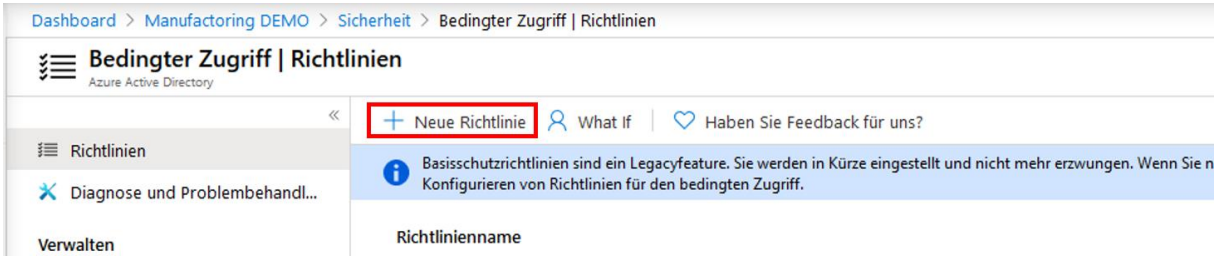


Abbildung 8: Erstellen einer neuen Richtlinie/Policy für den bedingten Zugriff

In diesem Beispiel wird mithilfe einer Richtlinie für alle Benutzer für jeden Zugriff MFA verlangt. Diese Richtlinie stellt die empfohlene Variante zur oben genannten MFA-Aktivierung dar.

Abhängig von weiteren Lizenzen (AAD P2, MCAS) haben Sie weitere Einstellungsmöglichkeiten. Für das MFA-Beispiel müssen drei Optionen konfiguriert werden:

1. Benutzer und Gruppen: Wählen Sie hier eine definierte Gruppe oder alle Benutzer aus, für die MFA aktiviert werden soll.
   Wichtig: Wenn Sie alle Benutzer inkludieren, wird empfohlen, einen dedizierten Backup-Benutzer auszuschließen, für den Fall, dass Sie sich mit Conditional Access ausgesperrt haben. Der Backup-Benutzer sollte mindestens die Rechte für die Administration von Conditional Access innehaben und sicher verwahrt werden, beispielsweise in einem Safe. Dieser Benutzer ist nicht für die tägliche Benutzung gedacht.

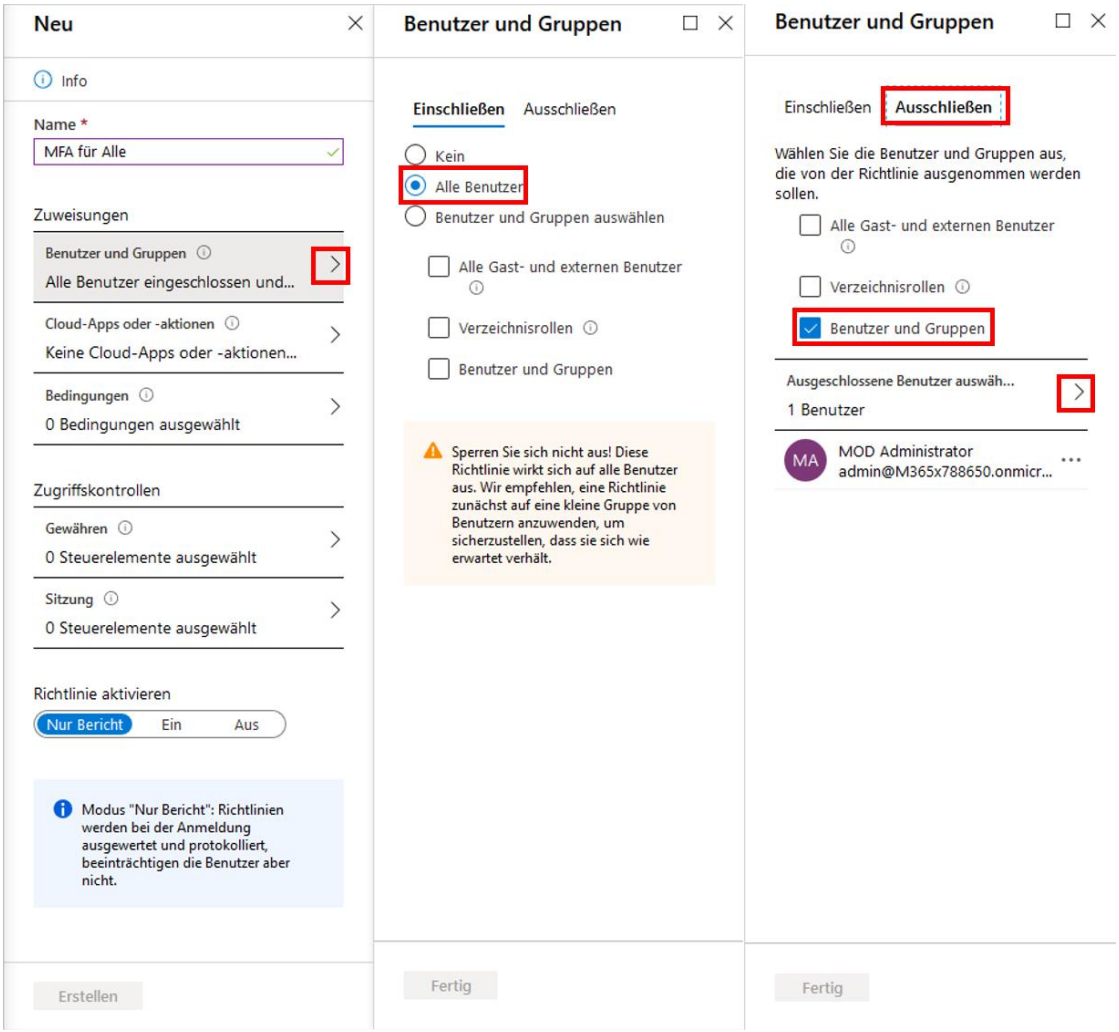


Abbildung 9: Konfigurieren einer Ausnahme für Richtlinien des bedingten Zugriffs

Siehe hierzu auch die Dokumentation zu Verwalten von Konten für den Notfallzugriff in Azure AD.

2. Cloud-Apps oder -aktionen: Wählen Sie hier alle Apps, die Sie inkludieren wollen:

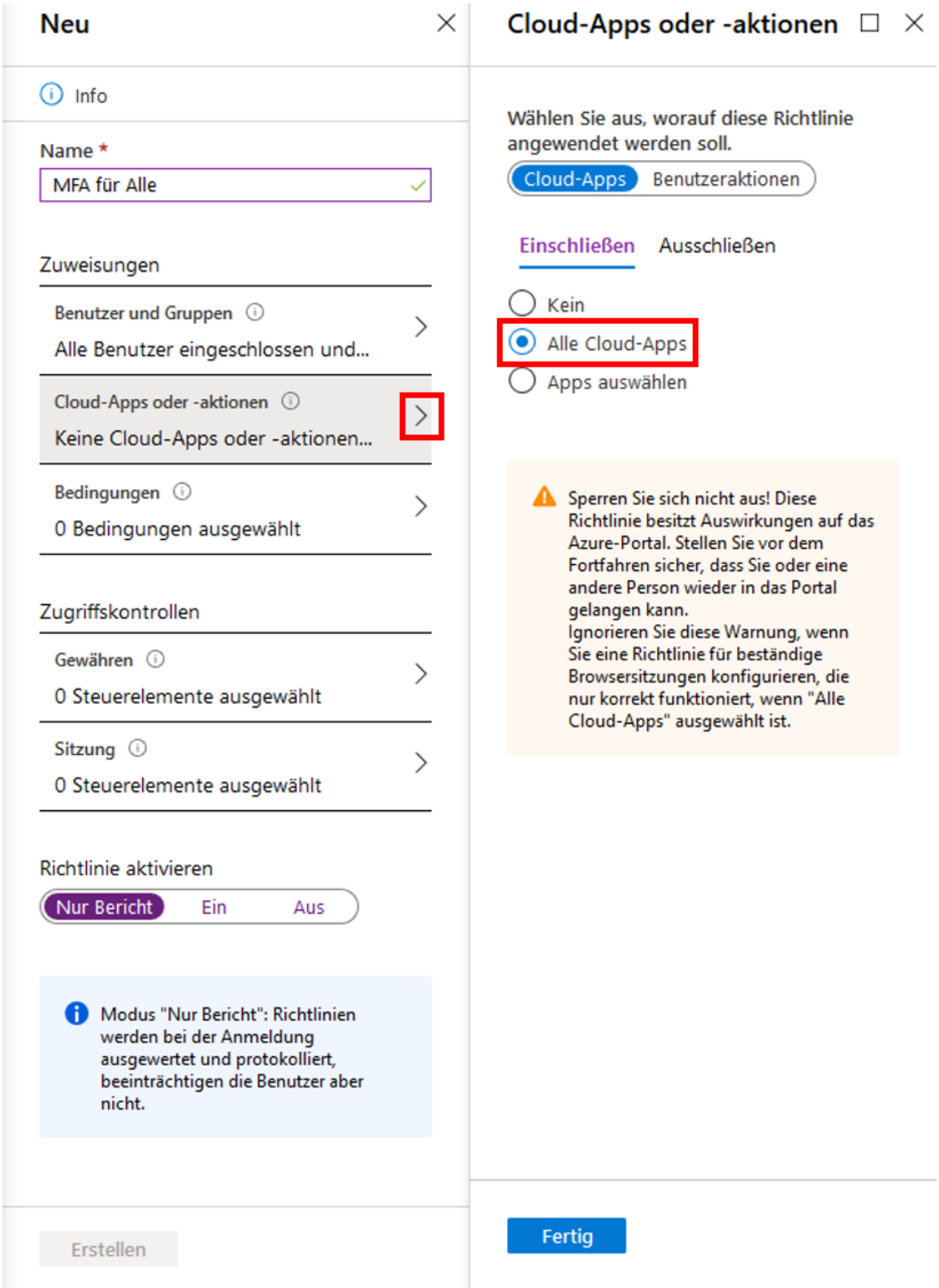


Abbildung 10: Zuweisen der Richtlinie für alle betroffenen Apps

3. Gewähren: Wählen Sie „Zugriff gewähren“ aus und aktivieren Sie zusätzlich den Punkt „Erfordert mehrstufige Authentifizierung“.

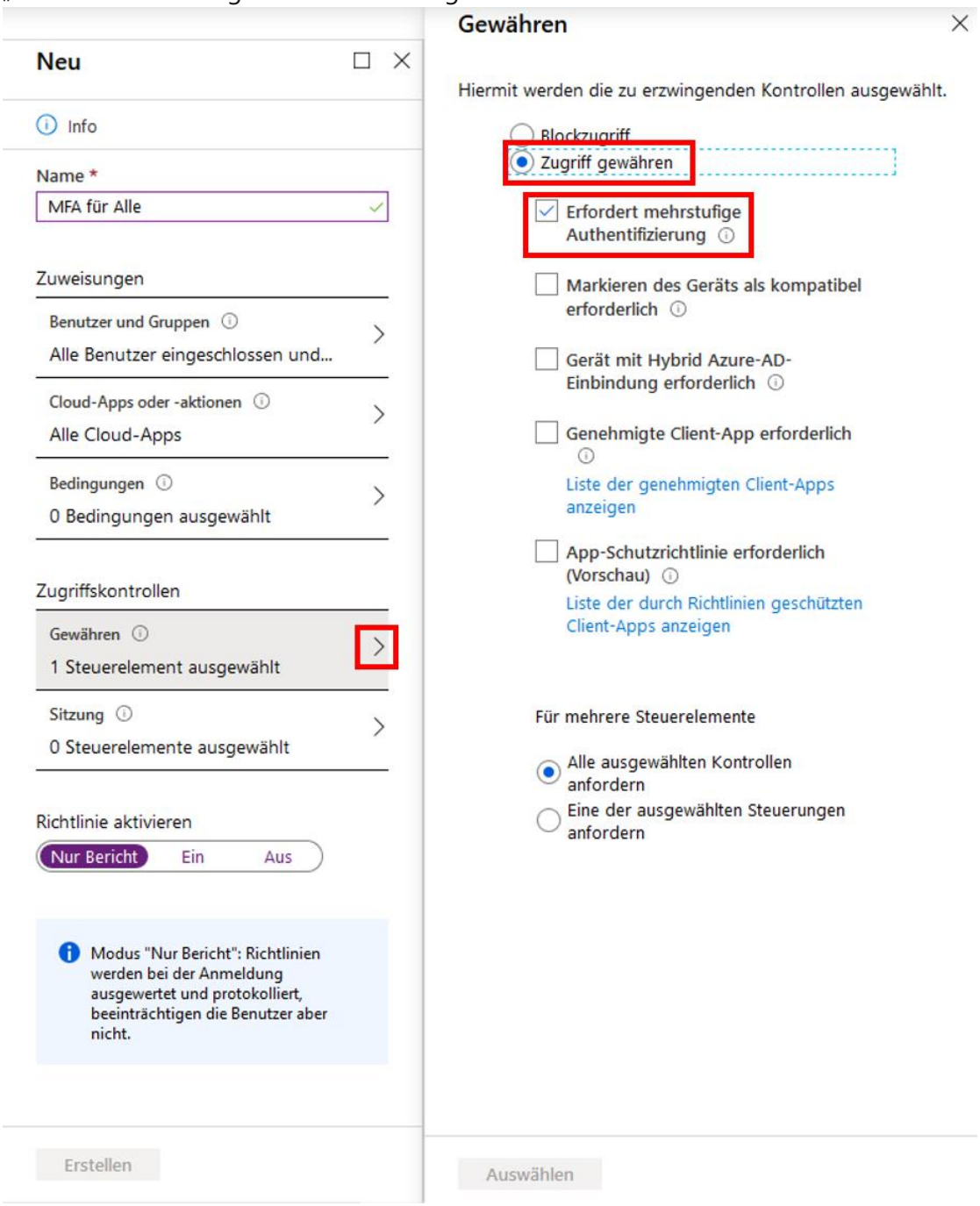


Abbildung 11: Einstellen der Voraussetzung für den erfolgreichen Zugriff

Klicken Sie zu guter Letzt auf „Richtlinie aktivieren – ein“ und anschließend auf „Erstellen“.

Dokumentbeginn

Self-Service Password Reset (SSPR)

Nachfolgend wird die anwenderseitige Kennwort-Rücksetzfunktion (Self-Service Password Reset) in Azure Active Directory beschrieben. Wenn ein Benutzer zum Kennwortzurücksetzungsportal navigiert, wird ein Workflow gestartet, um Folgendes zu bestimmen:

- Wie soll die Seite lokalisiert werden?
- Ist das Benutzerkonto gültig?
- Zu welcher Organisation gehört der Benutzer?
- Wo wird das Kennwort des Benutzers verwaltet?
- Ist der Benutzer zur Verwendung des Features lizenziert?

In den folgenden Schritten wird beschrieben, welche Logik hinter der Seite zur Kennwortzurücksetzung steckt:

1. Der Benutzer klickt auf den Link **Sie können nicht auf Ihr Konto zugreifen?** oder wechselt direkt zu https://aka.ms/sspr.
    - Die Benutzeroberfläche wird basierend auf dem Browsergebietsschema in der entsprechenden Sprache wiedergegeben. Die Benutzeroberfläche für das Zurücksetzen des Kennworts wird in alle Sprachen lokalisiert, die Office 365 unterstützt.
    - Wenn Sie das Portal für die Kennwortzurücksetzung in einer anderen Sprache anzeigen möchten, fügen Sie am Ende der URL für die Kennwortzurücksetzung „?mkt=“ ein, wie im folgenden Beispiel für Spanisch zu sehen:

      https://passwordreset.microsoftonline.com/?mkt=es-us

2. Der Benutzer gibt eine Benutzer-ID ein und durchläuft erfolgreich die Captchaprüfung.
3. Azure AD prüft folgendermaßen, ob der Benutzer diese Funktion verwenden darf:
    - Es wird geprüft, ob die Funktion für diesen Benutzer aktiviert ist und ob eine Azure AD-Lizenz zugewiesen ist.
        - Wenn diese Funktion für den Benutzer nicht aktiviert ist oder keine Lizenz vorliegt, wird der Benutzer aufgefordert, sich zum Zurücksetzen des Kennworts an den Administrator zu wenden.
    - Es wird überprüft, ob der Benutzer in seinem Konto die richtigen Authentifizierungsmethoden definiert hat, die der Administratorrichtlinie entsprechen.
        - Wenn die Richtlinie nur eine Methode erfordert, wird sichergestellt, dass der Benutzer für mindestens eine durch die Administratorrichtlinie aktivierte Authentifizierungsmethode geeignete Daten definiert hat.
        - Wenn die Authentifizierungsmethoden nicht konfiguriert sind, wird der Benutzer aufgefordert, sich an den Administrator zu wenden, um sein Kennwort zurückzusetzen.

        - Wenn die Richtlinie zwei Methoden erfordert, wird sichergestellt, dass der Benutzer für mindestens zwei durch die Administratorrichtlinie aktivierte Authentifizierungsmethoden geeignete Daten definiert hat.
        - Wenn die Authentifizierungsmethoden nicht konfiguriert sind, wird der Benutzer aufgefordert, sich an den Administrator zu wenden, um sein Kennwort zurückzusetzen.
        - Wenn einem Benutzer eine Azure-Administratorrolle zugewiesen wird, wird dadurch auch die sichere Zwei-Wege-Kennwortrichtlinie erzwungen. Weitere Informationen zu dieser Richtlinie finden Sie im Abschnitt Unterschiede zu Richtlinien zum Zurücksetzen von Administratorkennwörtern.
    - Es wird überprüft, ob das Benutzerkennwort lokal verwaltet wird (im Verbund, mit Pass-Through-Authentifizierung oder mit Kennwort-Hash-Synchronisierung).
        - Wenn das Rückschreiben von Kennwörtern konfiguriert ist und das Benutzerkennwort lokal verwaltet wird, kann der Benutzer mit der Authentifizierung fortfahren und sein Kennwort zurücksetzen.
        - Wenn das Rückschreiben von Kennwörtern nicht konfiguriert ist und das Benutzerkennwort lokal verwaltet wird, wird der Benutzer aufgefordert, sich zum Zurückzusetzen des Kennworts an den Administrator zu wenden.
4. Wenn festgestellt wird, dass der Benutzer sein Kennwort zurücksetzen darf, wird er durch den Vorgang für die Kennwortzurücksetzung geleitet.

Dokumentbeginn

Authentifizierungsmethoden

Wenn SSPR aktiviert ist, müssen Sie mindestens eine der folgenden Optionen als Authentifizierungsmethode auswählen. Es wird dringend empfohlen, **mindestens zwei Authentifizierungsmethoden** auszuwählen, damit Ihre Benutzer ausweichen können, falls sie auf eine Methode nicht zugreifen können. Weitere Informationen zu den unten aufgeführten Methoden finden Sie im Artikel Was sind Authentifizierungsmethoden?

- Benachrichtigung über eine mobile App
- Code der mobilen App
- E-Mail
- Mobiltelefon
- Bürotelefon
- Sicherheitsfragen

Benutzer können ihr Kennwort nur zurücksetzen, wenn für sie Daten in den Authentifizierungsmethoden vorliegen, die der Administrator aktiviert hat.

Zur Konfiguration der Authentifizierungsmethoden gehen Sie wie folgt vor:

Wählen Sie in Azure Active Directory „Zurücksetzen des Kennworts“ aus.

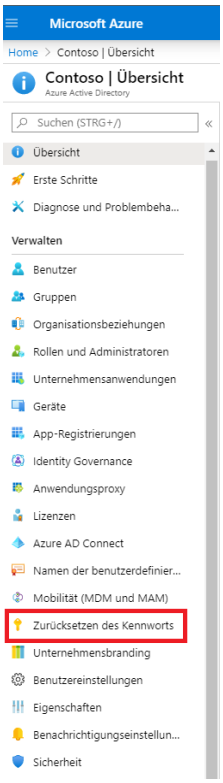


Abbildung 12: Administrative Konfiguration des SSPR

Unter „Eigenschaften“ wird die Funktion zum Zurücksetzen des Passwortes aktiviert und für alle Anwender oder nur einen Teil der Anwender innerhalb des Azure AD Tenants freigeschaltet. Das Beispiel zeigt eine Gruppe von Anwendern „SSPR Users“, die für diese Funktion berechtigt werden.

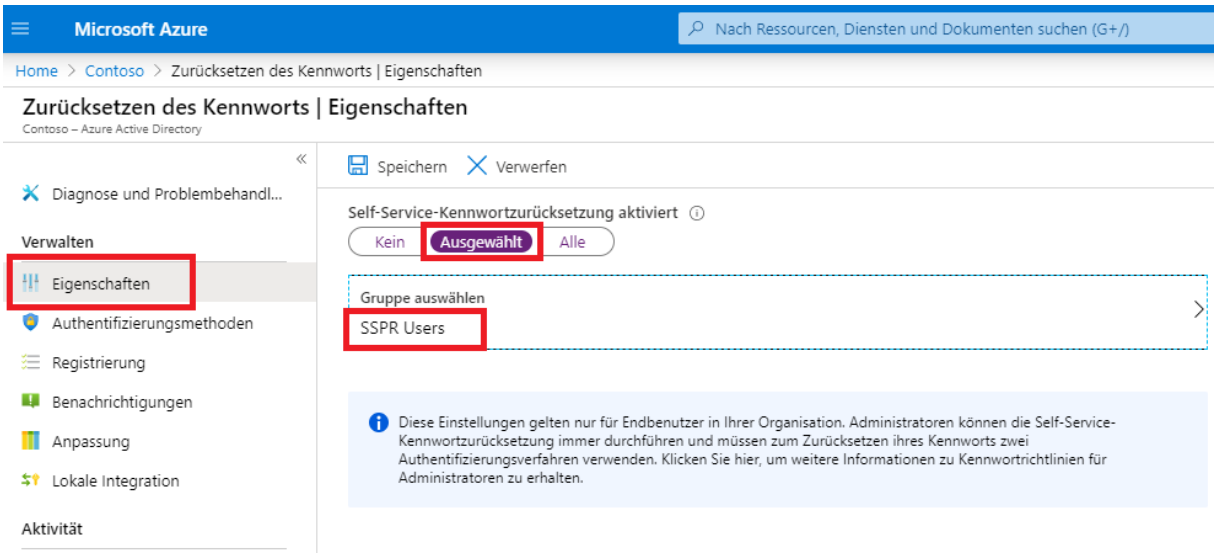


Abbildung 13: Zuweisen einer Gruppe zum SSPR

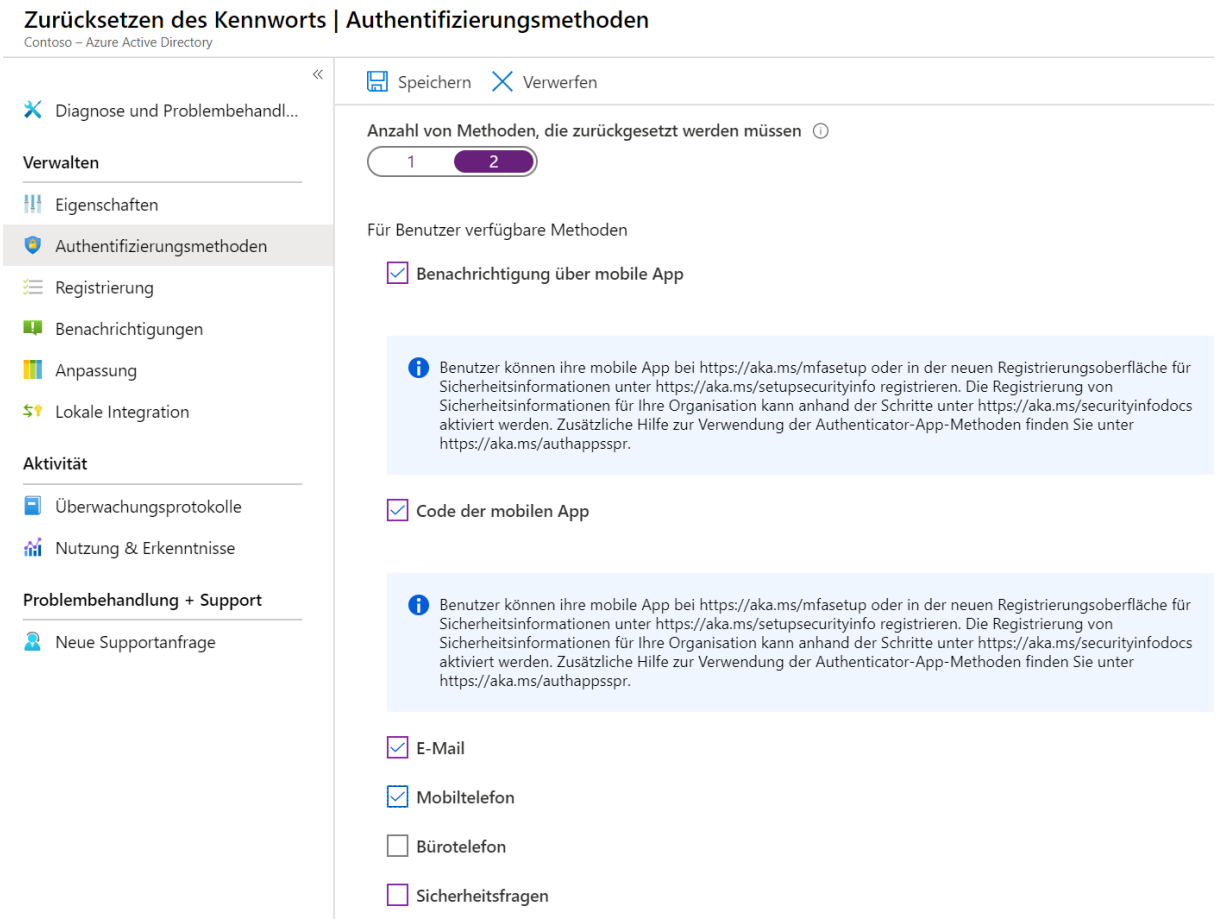


Abbildung 14: Einstellung der Möglichkeiten für ein SSPR

Wählen Sie, wie weiter oben beschrieben, Anzahl und Art der Authentifizierungsmöglichkeiten aus und bestätigen anschließend mit „Speichern“.

Lokale Integration

Wenn Sie Azure AD Connect installieren, konfigurieren und aktivieren, stehen folgende zusätzliche Optionen für lokale Integrationen zur Verfügung. Wenn diese Optionen abgeblendet sind, wurde das Rückschreiben nicht ordnungsgemäß konfiguriert. Weitere Informationen finden Sie unter Konfigurieren des Kennwortrückschreibens.

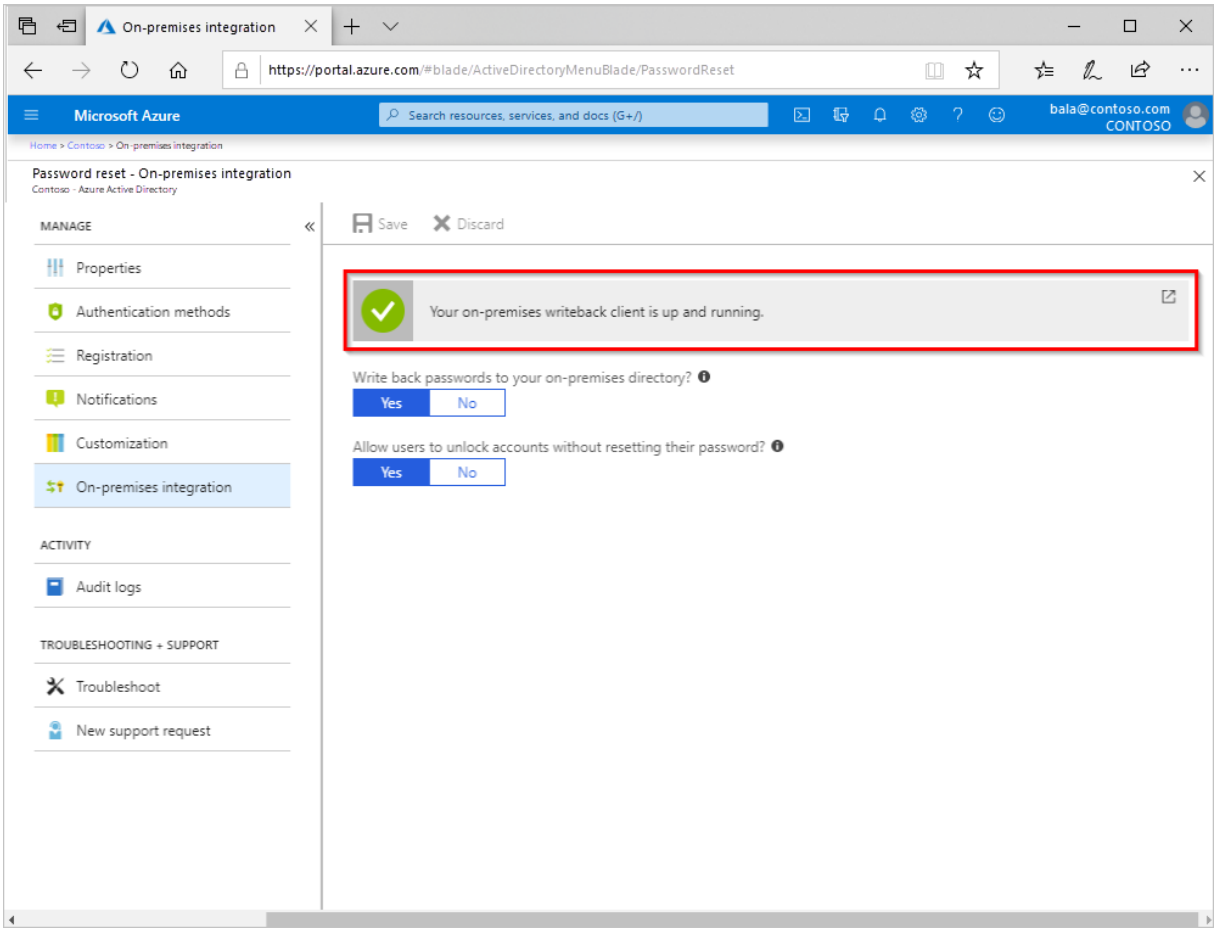


Abbildung 15: Integration des SSPR in das On-Premises Active Directory

Auf dieser Seite erhalten Sie einen schnellen Überblick über den Status des lokalen Clients für das Rückschreiben. Basierend auf der aktuellen Konfiguration wird eine der folgenden Meldungen angezeigt:

- Ihr lokaler Client für das Rückschreiben ist einsatzbereit.
- Azure AD Connect ist online und mit Ihrem lokalen Client für das Rückschreiben verbunden. Die installierte Version von Azure AD Connect ist jedoch offenbar veraltet. Ziehen Sie ein Upgrade von Azure AD Connect in Betracht, um sicherzustellen, dass Sie über die neuesten Konnektivitätsfeatures und wichtige Fehlerbehebungen verfügen.
- Leider können wir den Status Ihres lokalen Clients für das Rückschreiben nicht überprüfen, weil die installierte Version von Azure AD Connect nicht aktuell ist. Aktualisieren Sie Azure AD Connect, um den Verbindungsstatus überprüfen zu können.

- Leider können wir keine Verbindung mit Ihrem lokalen Client für das Rückschreiben herstellen. Führen Sie eine Problembehandlung für Azure AD Connect durch, um die Verbindung wiederherzustellen.
- Leider können wir keine Verbindung mit Ihrem lokalen Client für das Rückschreiben herstellen, weil das Kennwortrückschreiben nicht ordnungsgemäß konfiguriert wurde. Konfigurieren Sie das Kennwortrückschreiben, um die Verbindung wiederherzustellen.
- Leider können wir keine Verbindung mit Ihrem lokalen Client für das Rückschreiben herstellen. Möglicherweise liegen auf unserer Seite vorübergehende Probleme vor. Wenn das Problem weiterhin besteht, führen Sie eine Problembehandlung für Azure AD Connect durch, um die Verbindung wiederherzustellen.

Kennwörter in Ihr lokales Verzeichnis zurückschreiben
Dieses Steuerelement bestimmt, ob das Rückschreiben von Kennwörtern für dieses Verzeichnis aktiviert ist. Wenn das Rückschreiben aktiviert ist, gibt es den Status des lokalen Diensts für das Rückschreiben an. Dieses Steuerelement ist nützlich, wenn Sie das Kennwortrückschreiben vorübergehend deaktivieren möchten, ohne Azure AD Connect erneut zu konfigurieren.

- Wenn die Option auf **Ja** gesetzt ist, wird das Rückschreiben aktiviert, und Verbundbenutzer und Benutzer mit Pass-Through-Authentifizierung oder mit Kennwort-Hash-Synchronisierung können ihre Kennwörter zurücksetzen.
- Wenn die Option auf **Nein** gesetzt ist, wird das Rückschreiben deaktiviert, und Verbundbenutzer und Benutzer mit Pass-Through-Authentifizierung oder mit Kennwort-Hash-Synchronisierung können ihre Kennwörter nicht zurücksetzen.

Benutzern das Entsperren von Konten ohne Zurücksetzen des Kennworts erlauben
Dieses Steuerelement legt fest, ob Benutzer, die das Kennwortzurücksetzungsportal aufrufen, die Option zum Entsperren ihrer lokalen Active Directory-Konten ohne Zurücksetzen ihres Kennworts erhalten sollen. Standardmäßig werden bei einer Kennwortzurücksetzung Konten von Azure AD entsperrt. Mit dieser Einstellung können Sie diese beiden Vorgänge trennen.

- Bei der Einstellung **Ja** erhalten Benutzer die Option zum Zurücksetzen ihres Kennworts und Entsperren ihres Kontos oder die Option zum Entsperren des Kontos, ohne dass das Kennwort zurückgesetzt werden muss.
- Bei der Einstellung **Nein** können Benutzer das Entsperren des Kontos nur in Kombination mit dem Zurücksetzen des Kennworts vornehmen.

Lokaler Active Directory-Kennwortfilter
Die Azure AD-Self-Service-Kennwortzurücksetzung ist äquivalent zu einer vom Administrator ausgelösten Kennwortzurücksetzung in Active Directory. Wenn Sie einen Kennwortfilter eines Drittanbieters verwenden, um benutzerdefinierte Kennwortrichtlinien durchzusetzen, und Sie die Überprüfung dieses Kennwortfilters während der Azure AD-Self-Service-Kennwortzurücksetzung als erforderlich festlegen, müssen Sie sicherstellen, dass der

Kennwortfilter des Drittanbieters so konfiguriert ist, dass er im Szenario der Kennwortzurücksetzung durch den Administrator angewendet wird. Der Azure AD-Kennwortschutz für Windows Server Active Directory wird standardmäßig unterstützt.

Die nächsten Schritte

Die folgenden Artikel führen zu weiteren Informationen zur Kennwortzurücksetzung mit Azure AD:

- Erfolgreiches Rollout der Self-Service-Kennwortzurücksetzung
- Zurücksetzen oder Ändern des Kennworts
- Registrieren für die Self-Service-Kennwortzurücksetzung
- Lizenzanforderungen für Azure AD-Self-Service-Kennwortzurücksetzung
- Bereitstellen der Kennwortzurücksetzung ohne erforderliche Endbenutzerregistrierung
- Authentifizierungsmethoden
- Kennwortrichtlinien und -einschränkungen in Azure Active Directory
- Übersicht über die Kennwortrückschreibung
- Berichterstellungsoptionen für die Kennwortverwaltung von Azure AD
- Welche Optionen sind für SSPR verfügbar, und was bedeuten sie?
- Anscheinend ist ein Fehler aufgetreten. Wie behebe ich Probleme mit SSPR?
- Ich habe eine Frage, die nicht an einer anderen Stelle abgedeckt wurde.

Dokumentbeginn

Azure Application Proxy

Der Application Proxy (im Folgenden Anwendungsproxy genannt) ist ein Feature von Azure AD, mit dem Benutzer von einem Remoteclient aus auf lokale Webanwendungen zugreifen können. Der Anwendungsproxy umfasst den Anwendungsproxy-Dienst, der in der Cloud ausgeführt wird, und den Anwendungsproxy-Connector, der auf einem lokalen Server ausgeführt wird. Azure AD, der Anwendungsproxy-Dienst und der Anwendungsproxy-Connector arbeiten zusammen, um Benutzeranmeldetoken sicher von Azure AD zur Webanwendung weiterzuleiten.

Der Anwendungsproxy funktioniert mit:

- Webanwendungen, für die zur Authentifizierung die integrierte Windows-Authentifizierung verwendet wird
- Webanwendungen mit formularbasiertem oder headerbasiertem Zugriff
- Web-APIs, die Sie für umfassende Anwendungen auf unterschiedlichen Geräten verfügbar machen möchten
- Hinter einem Remotedesktopgateway gehosteten Anwendungen
- Rich Client-Apps, die in der Active Directory-Authentifizierungsbibliothek (Active Directory Authentication Library, kurz ADAL) integriert sind

Der Anwendungsproxy unterstützt das einmalige Anmelden (Single Sign-on). Weitere Informationen zu unterstützten Methoden finden Sie unter Auswählen einer Methode für einmaliges Anmelden.

Der Anwendungsproxy wird empfohlen, um Remotebenutzern Zugriff auf interne Ressourcen zu gewähren. Der Anwendungsproxy ersetzt die Notwendigkeit eines VPN- oder Reverseproxys. Er ist nicht für interne Benutzer im Unternehmensnetzwerk bestimmt. Diese Benutzer, die den Anwendungsproxy unnötigerweise verwenden, können unerwartete und unerwünschte Leistungsprobleme verursachen.

Funktionsweise des Anwendungsproxys

Das folgende Diagramm zeigt, wie Azure AD und der Anwendungsproxy gemeinsam das einmalige Anmelden für lokale Anwendungen bereitstellen.

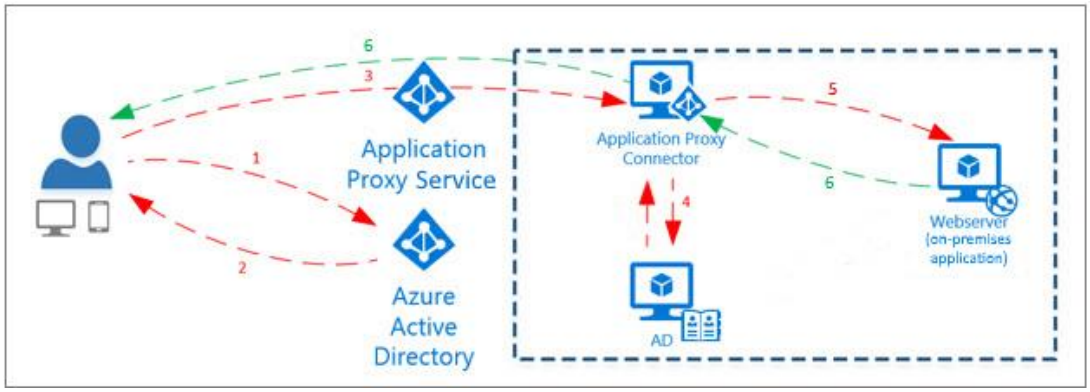


Abbildung 16: Funktionsweise des Anwendungsproxys

1. Nachdem der Benutzer über einen Endpunkt auf die Anwendung zugegriffen hat, wird er an die Azure AD-Anmeldeseite umgeleitet.
2. Nach der erfolgreichen Anmeldung sendet Azure AD ein Token an das Clientgerät des Benutzers.
3. Der Client sendet das Token an den Anwendungsproxy-Dienst, der den Benutzerprinzipalnamen (UPN) und den Sicherheitsprinzipalnamen (SPN) aus dem Token abruft. Der Anwendungsproxy sendet die Anforderung dann zum Anwendungsproxy-Connector.
4. Wenn Sie SSO konfiguriert haben, führt der Connector jede weitere erforderliche Authentifizierung im Namen des Benutzers durch.
5. Der Connector sendet die Anforderung an die lokale Anwendung.
6. Die Antwort wird über den Connector und den Anwendungsproxy-Dienst an den Benutzer gesendet.

Tabelle 4: Komponenten des Anwendungsproxys

Komponente	**Beschreibung**
Endpunkt	Der Endpunkt ist eine URL oder ein Endbenutzerportal. Benutzer können außerhalb Ihres Netzwerks über eine externe URL auf Anwendungen zugreifen. Benutzer in Ihrem Netzwerk können über eine URL oder ein Endbenutzerportal auf die Anwendung zugreifen. Wenn Benutzer einen dieser Endpunkte erreichen, authentifizieren sie sich in Azure AD und werden dann über den Connector an die lokale Anwendung geleitet.
Azure AD	Azure AD führt die Authentifizierung mit dem Mandantenverzeichnis aus, das in der Cloud gespeichert ist.
Anwendungsproxy-Dienst	Dieser Anwendungsproxy-Dienst wird in der Cloud als Teil von Azure AD ausgeführt. Er übergibt das Anmeldetoken des Benutzers an den Anwendungsproxy-Connector. Der Anwendungsproxy leitet alle in der Anforderung verfügbaren Header weiter und legt die Header gemäß seinem Protokoll auf die Client-IP-Adresse fest. Enthält die eingehende Anforderung an den Proxy bereits diesen Header, wird die Client-IP-Adresse am Ende der durch Trennzeichen getrennten Liste hinzugefügt, die der Wert des Headers ist.
Anwendungsproxy-Connector	Der Connector ist ein einfacher Agent, der auf einem Windows-Server innerhalb Ihres Netzwerks ausgeführt wird. Der Connector verwaltet die Kommunikation zwischen dem Anwendungsproxy-Dienst in der Cloud und der lokalen Anwendung. Der Connector verwendet nur ausgehende Verbindungen. Sie müssen also keine eingehenden Ports öffnen oder Ressourcen in die DMZ einfügen. Connectors sind zustandslos und rufen alle Informationen nach Bedarf aus der Cloud ab. Weitere Informationen zu Connectors, zum Beispiel wie der Lastenausgleich und die

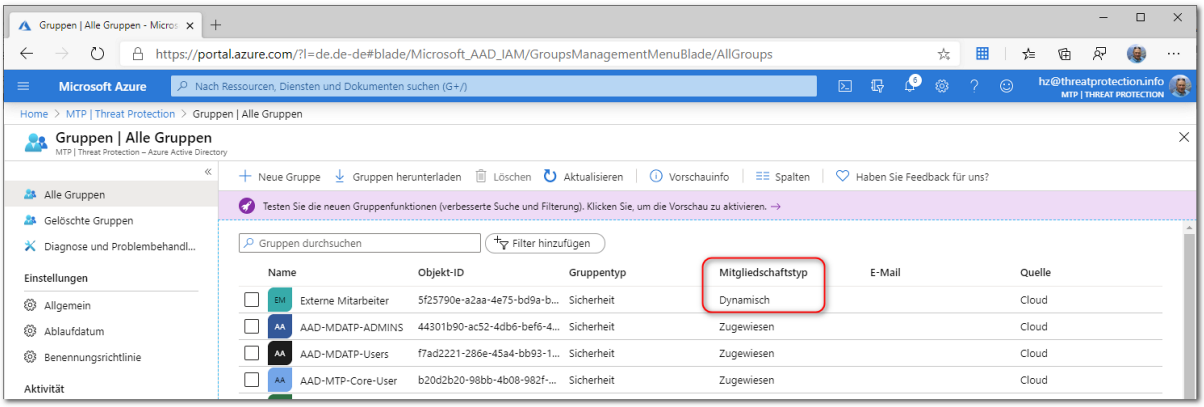
	Authentifizierung funktioniert, finden Sie unter Grundlegendes zu Azure AD-Anwendungsproxy-Connectors.
Active Directory (AD)	Active Directory wird lokal ausgeführt, um die Authentifizierung für Domänenkonten durchzuführen. Wenn einmaliges Anmelden konfiguriert ist, kommuniziert der Connector mit AD, um jede weitere erforderliche Authentifizierung auszuführen.
Lokale Anwendung	Schließlich kann der Benutzer auf eine lokale Anwendung zugreifen.

Weitere Schritte:
Planen der Bereitstellung eines Azure AD-Anwendungsproxys

Dokumentbeginn

Dynamische Gruppenmitgliedschaften

In Azure AD können Sie mithilfe von Regeln die Gruppenmitgliedschaft auf der Grundlage von Benutzer- oder Geräteeigenschaften festlegen. Dynamische Gruppenmitgliedschaften ermöglicht Ihnen schnelle und sichere Zuweisungen von Benutzern und Geräten in Gruppen.



Erstellen oder Aktualisieren einer dynamischen Gruppe in Azure Active Directory

Die dynamische Mitgliedschaft wird für den Gruppentyp **Sicherheit** und **Office 365** unterstützt. Wenn sich ein Attribut für einen Benutzer oder ein Gerät ändert, werden alle dynamischen Gruppenregeln in der Organisation verarbeitet, um Mitgliedschaftsänderungen zu berücksichtigen.

Benutzer und Geräte werden hinzugefügt oder entfernt, wenn sie die Bedingungen für eine Gruppe erfüllen. Sicherheitsgruppen können für Geräte oder Benutzer verwendet werden, Office 365-Gruppen dagegen können **nur** Benutzergruppen sein.

Regel-Generator im Azure Portal

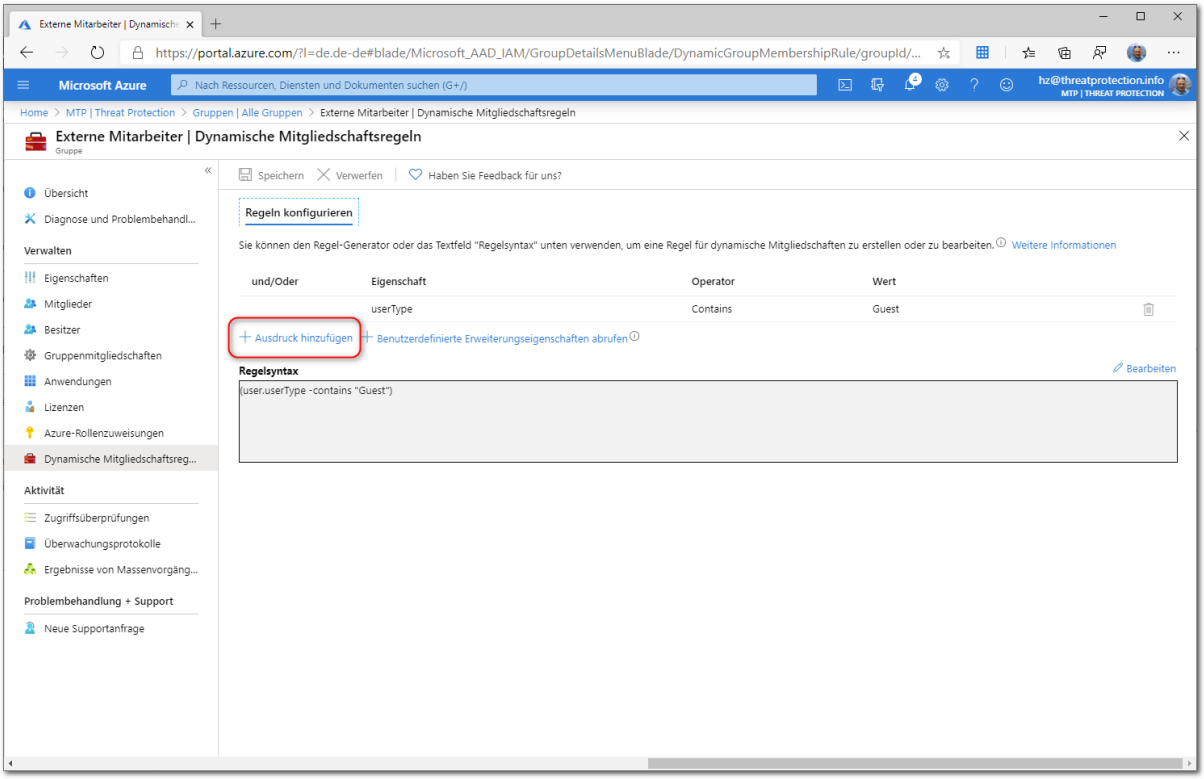
Azure AD stellt einen Regel-Generator bereit, mit dem Sie wichtige Regeln schneller erstellen und aktualisieren können. Der Regel-Generator unterstützt bei der Erstellung von bis zu fünf Ausdrücken. Die Erstellung einer Regel mit einigen einfachen Ausdrücken wird durch den Regel-Generator vereinfacht, aber er kann nicht verwendet werden, um jede Regel zu reproduzieren. Falls der Regel-Generator die zu erstellende Regel nicht unterstützt, können Sie das Textfeld verwenden.

Hier einige Beispiele, die für die Erstellung über das Textfeld empfohlen werden:

- Regel mit mehr als fünf Ausdrücken
- Mitarbeiterregel
- Festlegen der Rangfolge der Operatoren
- Regeln mit komplexen Ausdrücken, zum Beispiel
  `(user.proxyAddresses -any (_ -contains "contoso"))`

Hinweis

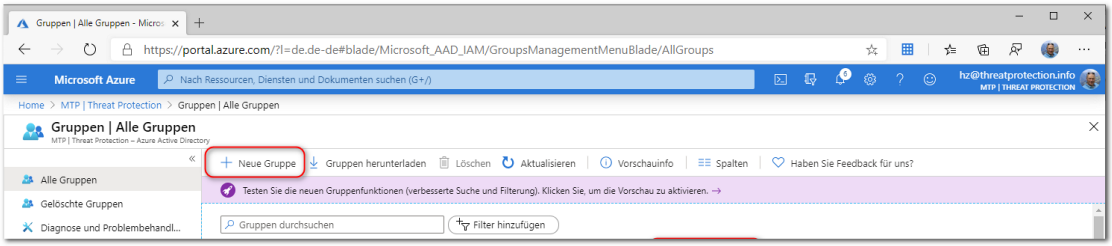
Der Regel-Generator kann gegebenenfalls einige Regeln, die über das Textfeld erstellt wurden, nicht anzeigen. Unter Umständen wird eine Meldung angezeigt, falls die Regel vom Regel-Generator nicht angezeigt werden kann. Der Regel-Generator nimmt keinerlei Änderungen an der unterstützten Syntax, Überprüfung oder Verarbeitung von Regeln für dynamische Gruppen vor.



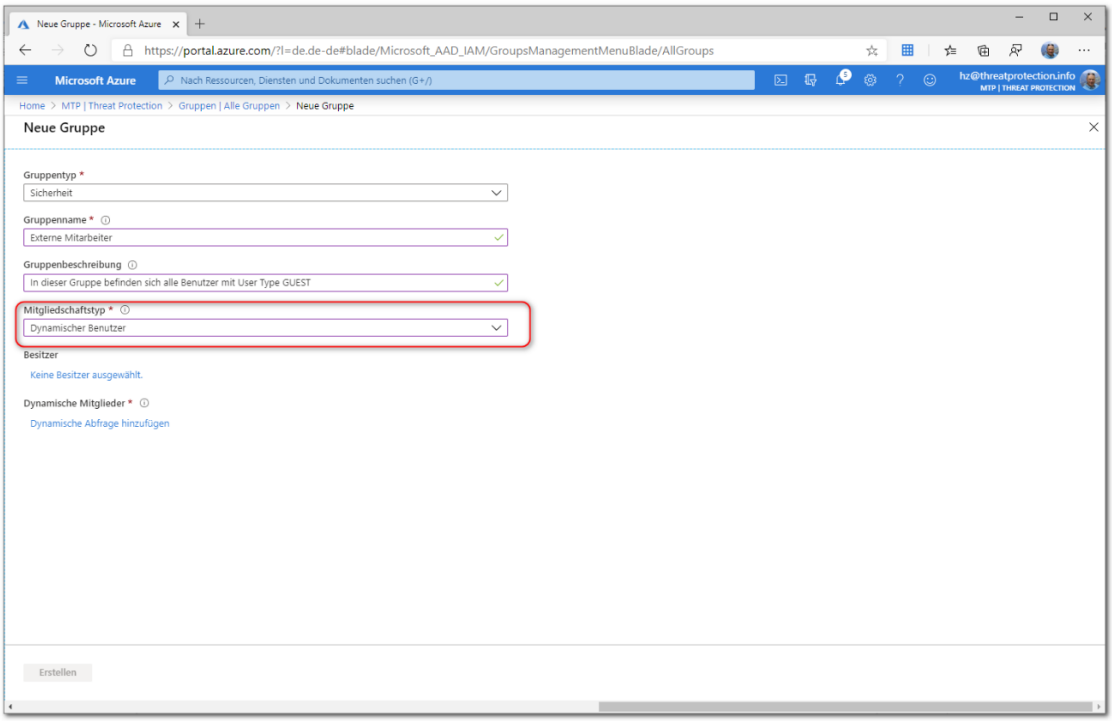
Beispiele für Syntax, unterstützte Eigenschaften, Operatoren und Werte für eine Mitgliedschaftsregel finden Sie unter [Regeln für eine dynamische Mitgliedschaft für Gruppen in Azure Active Directory].

So erstellen Sie eine Regel für die Gruppenmitgliedschaft:

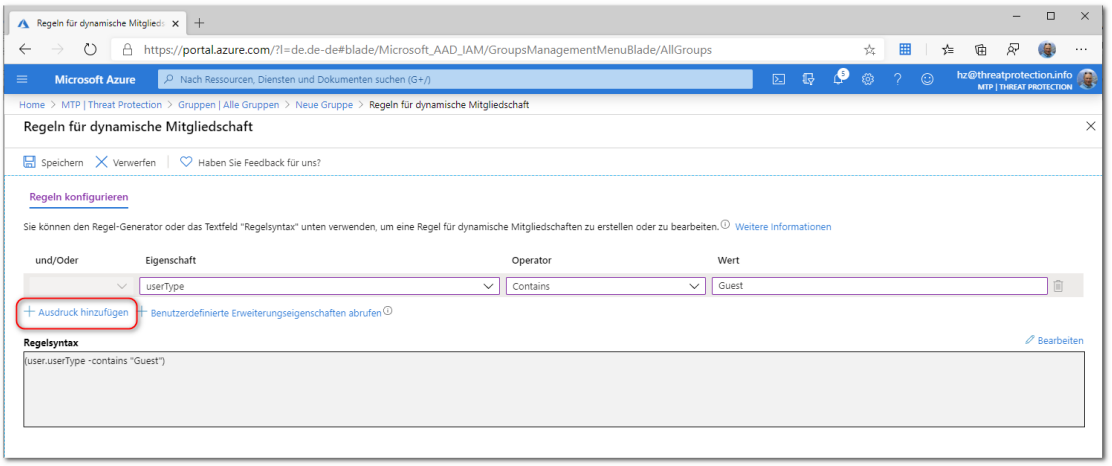
1. Melden Sie sich beim [Azure AD Admin Center] mit einem Konto an, das der Rolle des globalen Administrators, Intune-Administrators oder Benutzeradministrators in dem Mandanten angehört.
2. Suchen Sie nach „**Gruppen**“, und wählen Sie diese Option aus.
3. Wählen Sie unter „**Alle Gruppen**“ die Option „**Neue Gruppe**“ aus.



4. Geben Sie auf der Seite „**Neue Gruppe“** einen Namen und eine Beschreibung für die neue Gruppe ein. Wählen Sie unter „**Mitgliedschaftstyp“ die Option „D**ynamischer Benutzer“ oder „Geräte“ aus.



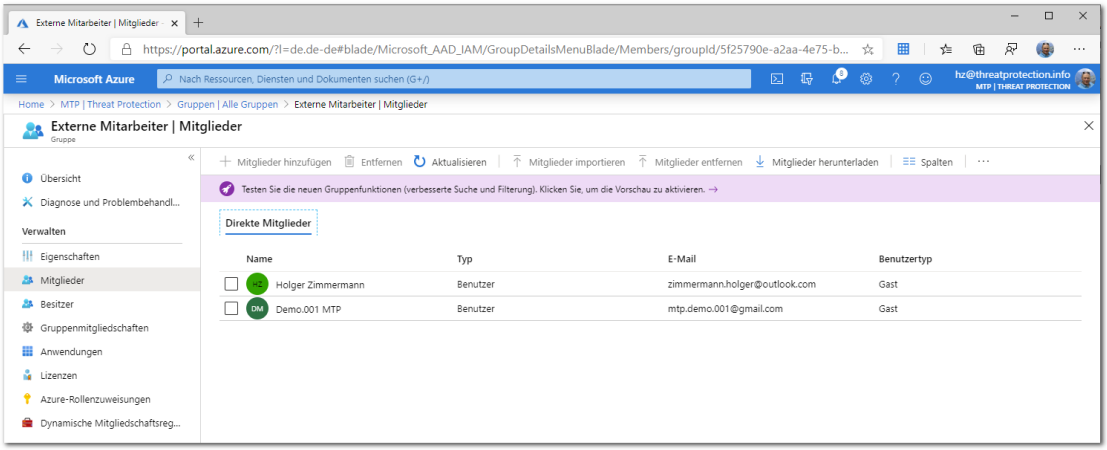
5. Klicken Sie auf „Dynamische Abfrage hinzufügen“.
6. Der Regel-Generator unterstützt bis zu fünf Ausdrücke. Falls Sie mehr als fünf Ausdrücke hinzufügen möchten, müssen Sie das Textfeld verwenden.



7. Klicken Sie nach dem Erstellen der Regel auf „**Speichern**“.

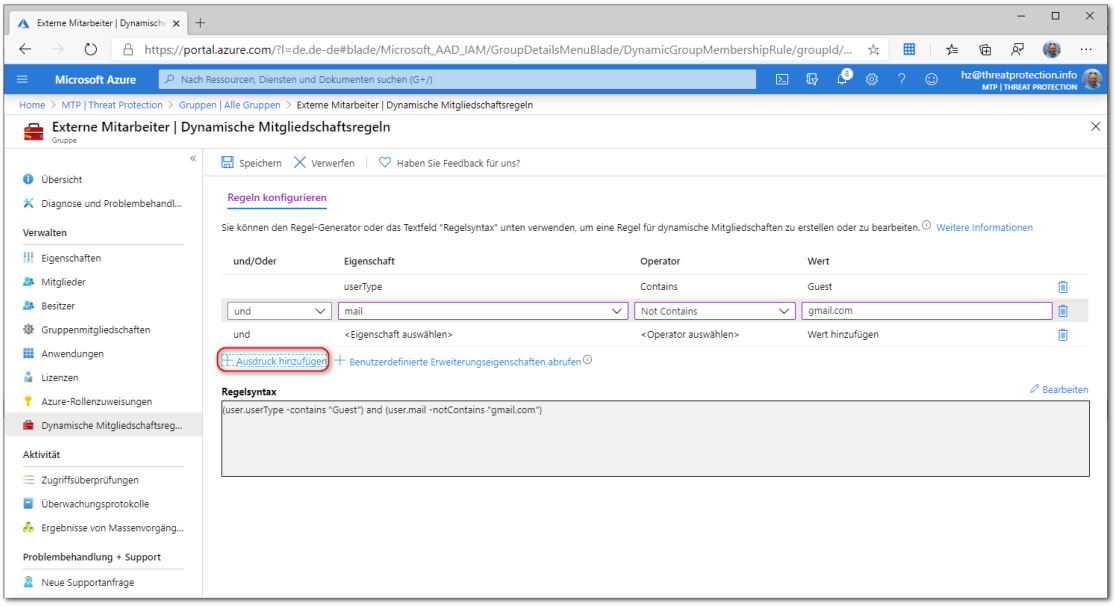
   Sollte die eingegebene Regel ungültig sein, wird über eine Azure-Benachrichtigung im Portal angezeigt, warum die Regel nicht verarbeitet werden konnte. Lesen Sie sich die Erklärung aufmerksam durch, um die Regel korrigieren zu können.

8. Unter der Option „Mitglieder“ können Sie alle Mitglieder, basierend auf dem Filter, anzeigen.

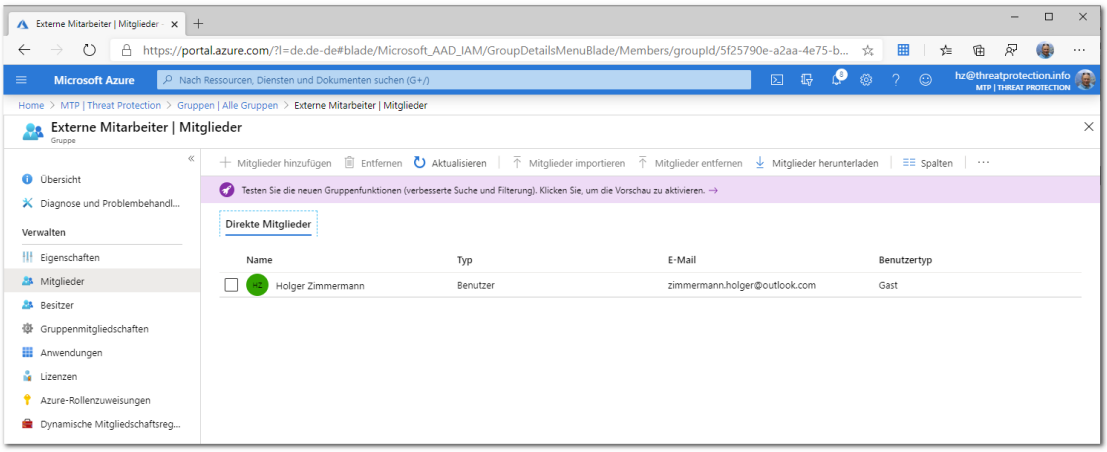


Aktualisieren einer vorhandenen Regel

1. Melden Sie sich beim Azure AD Admin Center mit einem Konto an, das der Rolle „Globaler Administrator“, „Gruppenadministrator“, „Intune-Administrator“ oder „Benutzeradministrator“ in dem Mandanten angehört.
2. Wählen Sie **Gruppen → Alle Gruppen** aus.
3. Wählen Sie eine Gruppe aus, um ihr Profil zu öffnen.
4. Wählen Sie auf der Profilseite für die Gruppe „**Dynamische Mitgliedschaftsregeln“** aus.
5. Fügen Sie einen weiteren Ausdruck hinzu beziehungsweise ändern oder löschen Sie einen vorhandenen Ausdruck. In diesem Beispiel wurde ein weiterer Ausdruck für das Attribute *user.mail* hinzugefügt:



6. Klicken Sie nach dem Aktualisieren der Regel auf „**Speichern**“.
7. Unter der Option „Mitglieder“ werden nun die geänderten Mitglieder, basierend auf dem neuen Filter, aufgelistet.



Dokumentbeginn

Gruppenbasierte Lizenzierung

Für kostenpflichtige Microsoft-Clouddienste wie Office 365, Enterprise Mobility + Security, Dynamics 365 und ähnliche Produkte werden Lizenzen benötigt. Diese Lizenzen werden jedem Benutzer zugewiesen, der Zugriff auf diese Dienste benötigt. Administratoren verwalten Lizenzen über eines der Verwaltungsportale (Office, Azure) und PowerShell-Cmdlets. Azure Active Directory ist die zugrunde liegende Infrastruktur, die die Identitätsverwaltung aller Microsoft Cloud-Dienste unterstützt. Azure AD speichert Informationen zum Lizenzzuweisungsstatus für Benutzer.

Bislang konnten Lizenzen nur auf Ebene einzelner Benutzer zugewiesen werden, was die umfassende Verwaltung erschweren kann. Um Benutzerlizenzen basierend auf Organisationsänderungen zu vergeben oder zu entziehen, wenn beispielsweise Benutzer der Organisation oder Abteilung beitreten oder diese verlassen, muss ein Administrator häufig ein komplexes PowerShell-Skript schreiben. Dieses Skript richtet einzelne Aufrufe an den Clouddienst.

Um diese Probleme zu beheben, enthält Azure AD jetzt die gruppenbasierte Lizenzierung. Sie können einer Gruppe eine oder mehrere Produktlizenzen zuweisen. Azure AD stellt sicher, dass die Lizenzen allen Mitgliedern der Gruppe zugewiesen werden. Allen neuen Mitgliedern, die der Gruppe beitreten, werden die entsprechenden Lizenzen zugewiesen. Wenn sie die Gruppe verlassen, werden diese Lizenzen entfernt. Dadurch ist keine automatisierte Lizenzverwaltung über PowerShell mehr erforderlich, um Änderungen in der Organisations- und Abteilungsstruktur benutzerbezogen widerzuspiegeln.

Hauptmerkmale der gruppenbasierten Lizenzierung:

- Lizenzen können beliebigen Sicherheitsgruppen in Azure AD zugewiesen werden. Sicherheitsgruppen können mithilfe von Azure AD Connect aus einer lokalen Umgebung synchronisiert werden. Sie können Sicherheitsgruppen auch direkt in Azure AD Connect (auch als reine Cloudgruppen bezeichnet) oder automatisch über das Azure AD-Feature „Dynamische Gruppe“ erstellen.
- Wenn eine Produktlizenz einer Gruppe zugewiesen wird, kann der Administrator einen oder mehrere Servicepläne im Produkt deaktivieren. In der Regel erfolgt diese Zuweisung, wenn die Organisation einen in einem Produkt enthaltenen Dienst noch nicht verwenden kann. Beispielsweise könnte der Administrator Office 365 einer Abteilung zuweisen, aber den Yammer-Dienst vorübergehend deaktivieren.
- Alle Microsoft-Clouddienste, die eine Lizenzierung auf Benutzerebene erfordern, werden unterstützt. Dazu zählen alle Office 365-Produkte, Enterprise Mobility + Security und Dynamics 365.
- Die gruppenbasierte Lizenzierung ist derzeit nur über das Azure Portal verfügbar. Wenn Sie in erster Linie andere Verwaltungsportale für die Benutzer- und Gruppenverwaltung nutzen, zum Beispiel das Microsoft 365 Admin Center, können Sie dies weiterhin tun. Jedoch sollten Sie das Azure Portal zum Verwalten von Lizenzen auf Gruppenebene verwenden.

- Azure AD verwaltet Lizenzänderungen, die sich aus Änderungen an der Gruppenmitgliedschaft ergeben, automatisch. In der Regel erfolgen Änderungen des Lizenzstatus binnen Minuten nach einer Mitgliedschaftsänderung.
- Ein Benutzer kann Mitglied mehrerer Gruppen mit angegebenen Lizenzrichtlinien sein. Ein Benutzer kann auch über Lizenzen verfügen, die außerhalb von Gruppen zugewiesen wurden. Der resultierende Benutzerstatus ist eine Kombination aller zugewiesenen Produkt- und Dienstlizenzen. Wenn einem Benutzer die gleiche Lizenz aus mehreren Quellen zugewiesen wurde, wird die Lizenz nur einmal genutzt.
- In manchen Fällen können Benutzern keine Lizenzen zugewiesen werden. Mögliche Gründe sind das Fehlen verfügbarer Lizenzen im Mandanten oder in Konflikt stehende Dienste, die gleichzeitig zugewiesen wurden. Administratoren haben Zugriff auf Informationen zu Benutzern, für die Azure AD Gruppenlizenzen nicht vollständig verarbeiten konnte. Sie können anhand dieser Informationen Korrekturmaßnahmen vornehmen.

Zuweisen von Lizenzen zu Benutzern nach Gruppenmitgliedschaft in Azure AD
Schritt 1: Zuweisen der erforderlichen Lizenzen

1. Melden Sie sich mit einem Lizenzadministratorkonto beim Azure AD Admin Center an. Zum Verwalten von Lizenzen muss das Konto ein Lizenzadministrator, Benutzeradministrator oder globaler Administrator sein.
2. Wählen Sie „**Lizenzen“** aus, um eine Seite zu öffnen, auf der Sie alle lizenzierbaren Produkte im Mandanten anzeigen und verwalten können.
3. Wählen Sie unter „**Alle Produkte“** zum Beispiel Enterprise Mobility + Security E5 aus, indem Sie die Produktnamen auswählen. Wählen Sie oben auf der Seite „**Zuweisen“** aus, um die Zuweisung zu starten.

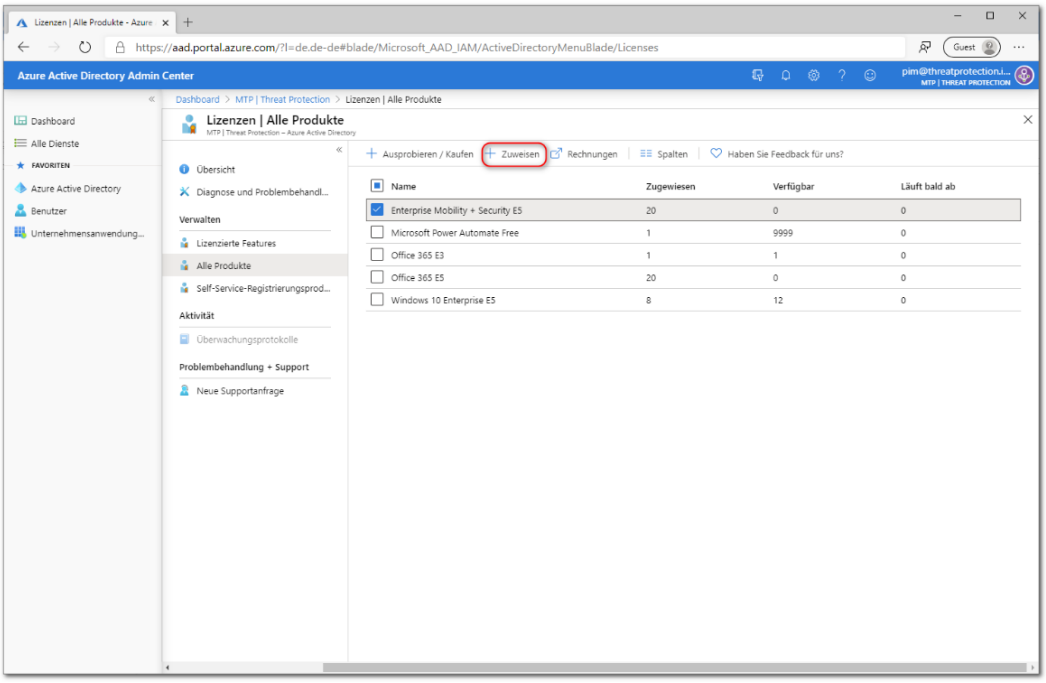


Abbildung 17: Zuweisen von Lizenzbundles im Azure Portal

4. Wählen Sie auf der Seite „**Lizenz zuweisen“** die Option „Benutzer und Gruppen“ aus, um eine Liste der Benutzer und Gruppen zu öffnen.
5. Wählen Sie einen Benutzer oder eine Gruppe aus, und bestätigen Sie Ihre Auswahl dann oben auf der Seite über die Schaltfläche „Auswählen“.
6. Klicken Sie auf der Seite „Lizenz zuweisen“ auf „Zuweisungsoptionen“. Daraufhin werden alle Workloads angezeigt, die in den zuvor ausgewählten Produkten enthalten sind. Aktivieren beziehungsweise deaktivieren Sie die entsprechenden Workloads. Bestätigen Sie den Vorgang, indem Sie unten in „Lizenzoptionen“ auf „OK“ klicken.

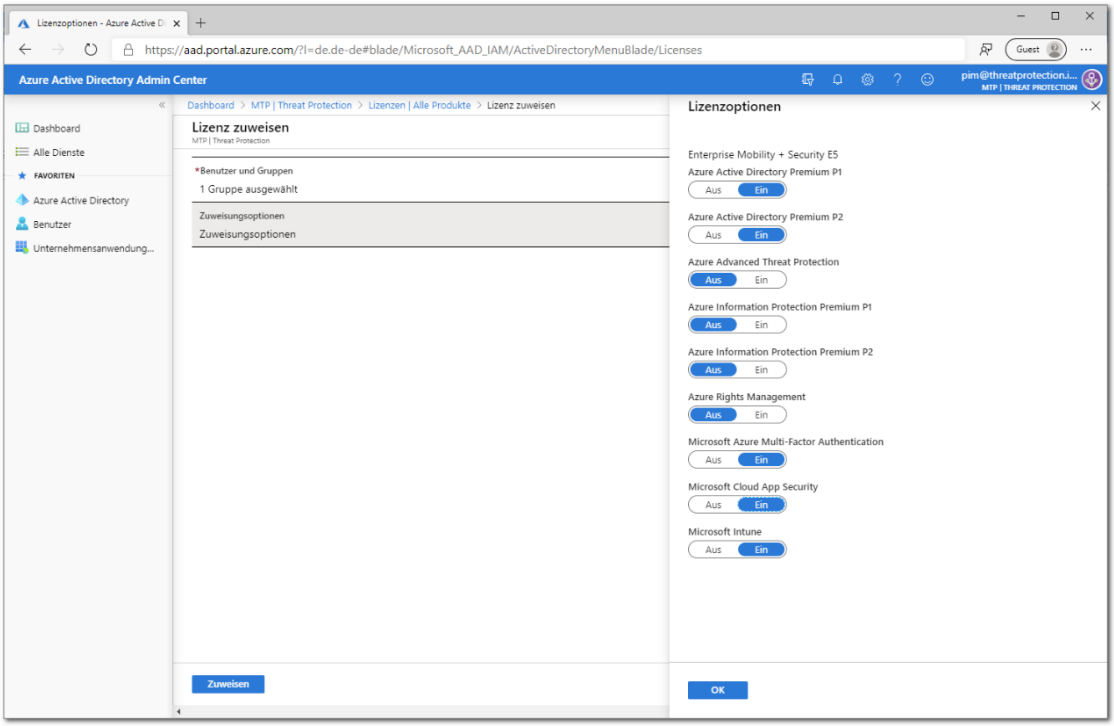


Abbildung 18: Dedizierte Zuweisung von einzelnen Lizenzprodukten

7. Klicken Sie schließlich unten auf der Seite „Lizenz zuweisen“ auf „Zuweisen“, um die Zuweisung abzuschließen.
8. Rechts oben wird eine Benachrichtigung mit dem Status und Ergebnis des Vorgangs angezeigt. Falls die Gruppenzuweisung nicht abgeschlossen werden konnte (beispielsweise aufgrund bereits vorhandener Lizenzen für die Gruppe), klicken Sie auf die Benachrichtigung, um Details zum Fehler anzuzeigen.

Beim Zuweisen von Lizenzen zu einer Gruppe werden in Azure AD alle vorhandenen Mitglieder dieser Gruppe verarbeitet. Je nach Größe der Gruppe kann dieser Vorgang einige Zeit dauern. Der nächste Schritt beschreibt, wie Sie überprüfen, ob der Vorgang abgeschlossen wurde und ob weitere Maßnahmen zur Problembehebung erforderlich sind.**Schritt 2: Überprüfen, ob die anfängliche Zuweisung erfolgt ist**

1. Wechseln Sie zu **Azure Active Directory → Gruppen**. Wählen Sie die Gruppe aus, der Lizenzen zugewiesen wurden.
2. Wählen Sie auf der Seite der Gruppe die Option „**Lizenzen“** aus. Dadurch können Sie schnell überprüfen, ob die Lizenzen den Benutzern vollständig zugewiesen wurden und

ob Fehler vorliegen, die untersucht werden müssen. Folgende Informationen stehen zur Verfügung:

a. Dienstlizenzen, die der Gruppe aktuell zugewiesen sind. Wählen Sie einen Eintrag aus, um die bestimmten Dienste anzuzeigen, die aktiviert wurden, und um Änderungen vorzunehmen.
b. Statusaktualisierungen der letzten Lizenzänderungen, die verfügbar sind, wenn die Änderungen verarbeitet werden oder wenn die Verarbeitung für alle Benutzermitglieder abgeschlossen ist.
c. Informationen zu Benutzerlizenzzuweisungen in einem Fehlerzustand.

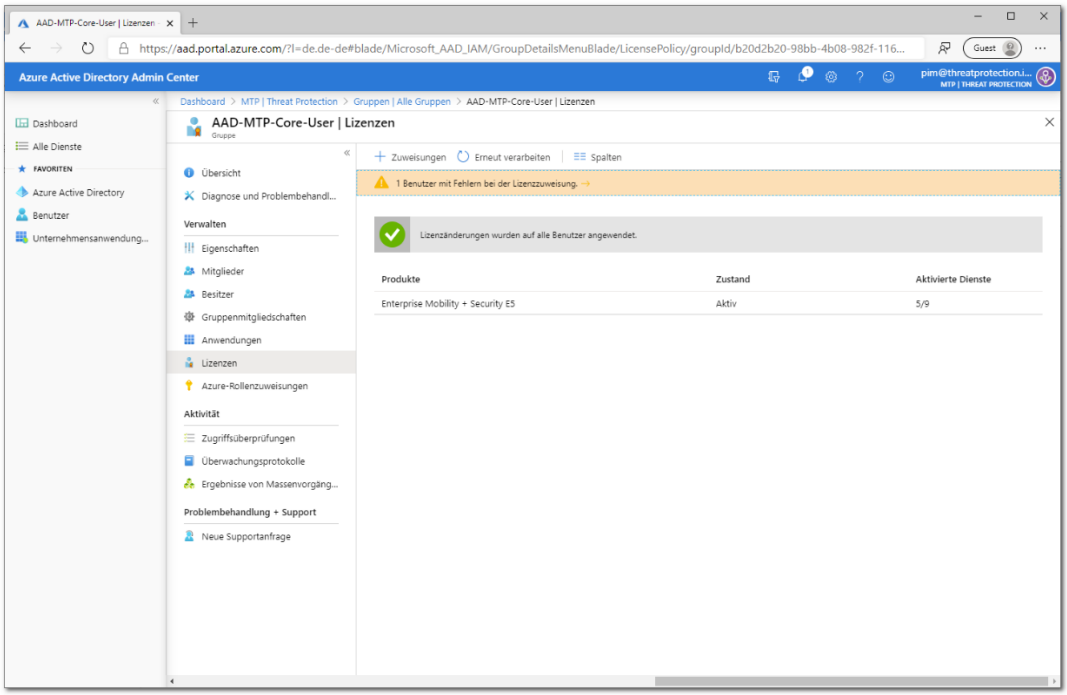


Abbildung 19: Fehlerzustand in der Lizenzübersicht

3. Ausführlichere Informationen zur Lizenzverarbeitung finden Sie unter **Azure Active Directory → Benutzer und Gruppen** → Gruppenname → **Überwachungsprotokolle**. Überprüfen Sie folgende Aktivitäten:

a. Aktivität: *Start applying group based license to users*. Wird protokolliert, wenn das System die Änderung der Lizenzzuweisung für die Gruppe verarbeitet und beginnt, diese für alle Benutzermitglieder zu übernehmen. Das Protokoll enthält Informationen über die erfolgte Änderung.
b. Aktivität: *Finish applying group based license to users*. Wird protokolliert, wenn das System alle Benutzer in der Gruppe verarbeitet hat. Das Protokoll enthält eine Übersicht über die Anzahl erfolgreich verarbeiteter Benutzer und über die Anzahl von Benutzern, denen keine Gruppenlizenzen zugewiesen werden konnten.

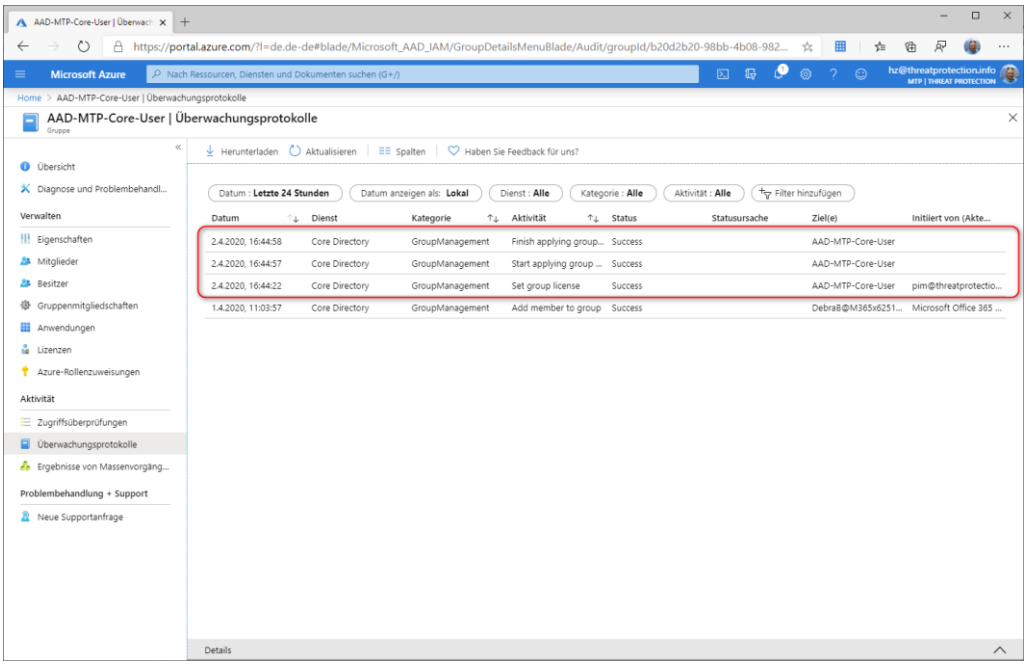


Abbildung 20: Informationen zum Zustand der Lizenzverwaltung im Überwachungsprotokoll

Weitergehende Informationen finden Sie auch in dem folgenden Abschnitt: Verwenden von Überwachungsprotokollen zum Überwachen von gruppenbasierten Lizenzierungsaktivitäten

Eine gruppenbasierte Lizenzierung kann selbstverständlich auf über ein dynamische Gruppenmitgliedschaft erfolgen. Siehe Erstellen oder Aktualisieren einer dynamischen Gruppe in Azure Active Directory.

Dokumentbeginn

Microsoft Intune

Microsoft Intune ist ein cloudbasierter Dienst, der sich auf die Verwaltung mobiler Geräte (MDM, Mobile Device Management) und mobiler Anwendungen (MAM, Mobile Application Management) konzentriert. Intune ermöglicht Benutzern mobiles und produktives Arbeiten bei gleichzeitigem Schutz der Unternehmensdaten. Intune ist nativ in Microsoft 365 und Azure Active Directory integriert und ermöglicht damit unter anderem feingranulare Zugriffssteuerung sowie Informationsschutz über Azure Information Protection.

Der Terminus „mobile Geräte“ inkludiert dabei explizit auch traditionelle Desktoprechner. Bei Organisationen mit großen lokalen Standorten ist die lokale Bereitstellung von Distributionsfunktionen nach wie vor empfehlenswert. Die nahtlose Integration von Microsoft Intune in Microsoft System Center Configuration Manager (SCCM) ermöglicht es Unternehmen, sämtliche Geräte in einer einzigen Konsole zu verwalten, und wird seit kurzem unter dem neuen Markennamen *Microsoft Endpoint Manager* geführt.

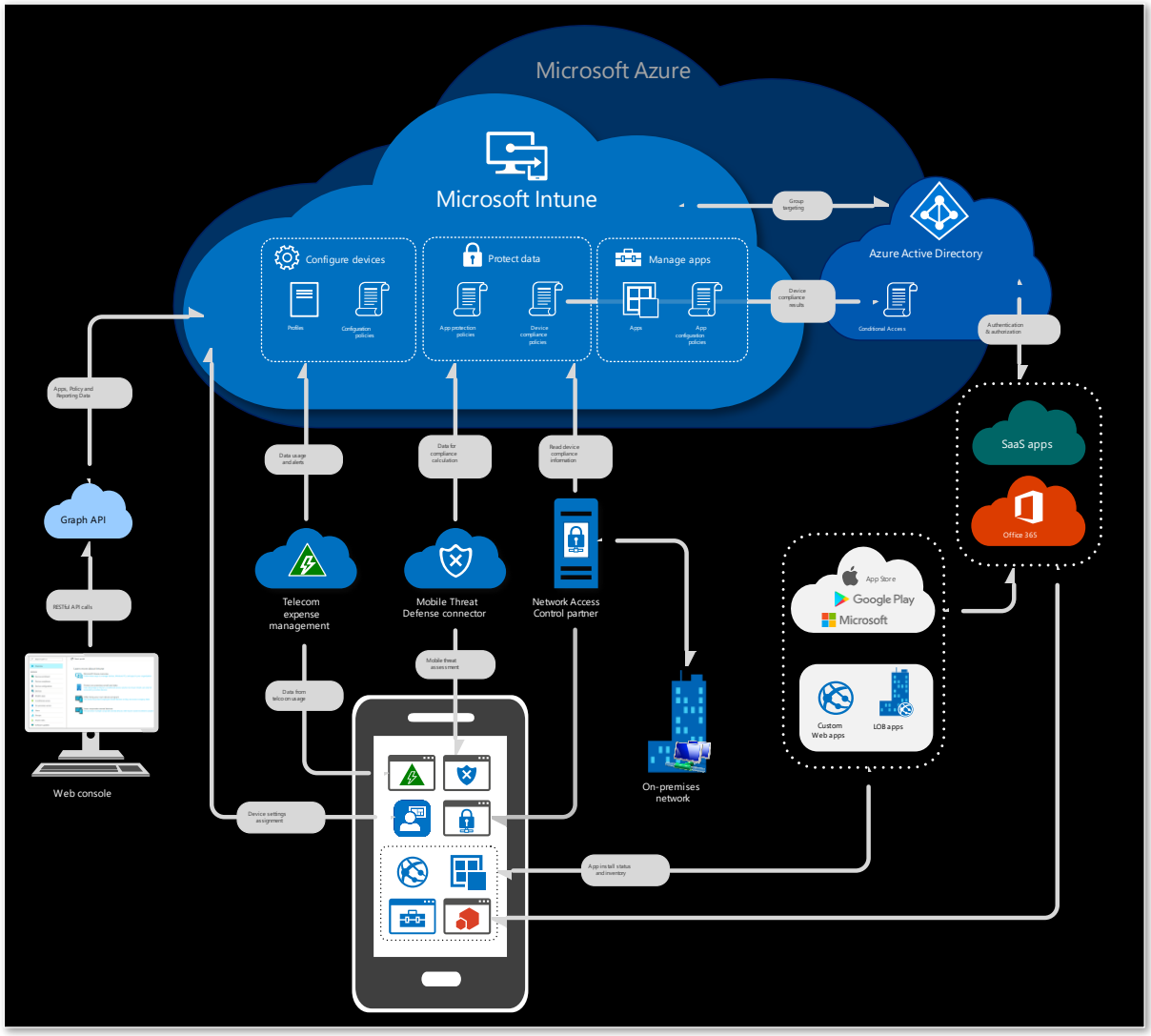


Abbildung 21: Schematische Darstellung der Zugriffe auf Microsoft Intune

Die folgenden Einrichtungsschritte helfen Ihnen, die mobile Geräteverwaltung (Mobile Device Management, MDM) mit Intune zu aktivieren. Geräte müssen verwaltet werden, bevor Sie Benutzern Zugriff auf Unternehmensressourcen gewähren oder Einstellungen auf diesen Geräten verwalten können.

Einige Schritte wie die Einrichtung eines Intune-Abonnements und der MDM-Autorität sind in den meisten Szenarien erforderlich. Andere Schritte wie das Konfigurieren einer benutzerdefinierten Domäne oder das Hinzufügen von Apps sind optional, je nach den Anforderungen Ihres Unternehmens. Wenn Sie Microsoft Configuration Manager derzeit zum Verwalten von Computern und Servern verwenden, können Sie Configuration Manager über die Co-Verwaltung mit der Cloud verknüpfen.

Unter bestimmten Voraussetzungen können Sie das ***FastTrack Center-Leistungsangebot*** nutzen. Bei diesem Dienst unterstützen Sie Microsoft-Spezialisten bei der Vorbereitung Ihrer Umgebung für Intune. Informationen hierzu finden Sie unter FastTrack Center-Leistungsangebot für Enterprise Mobility Suite (EMS).

Schritt	Aufgabe
1	Unterstützte Konfigurationen: Wichtige Informationen, bevor Sie beginnen. Dies beinhaltet die unterstützten Konfigurationen und Netzwerkanforderungen.
2	Anmelden bei Intune: Melden Sie sich bei Ihrem Testabonnement an, oder erstellen Sie ein neues Intune-Abonnement.
3	Konfigurieren des Domänennamens: Legen Sie die DNS-Registrierung fest, um den Domänennamen Ihres Unternehmens mit Intune zu verbinden. Dies bietet Benutzern eine vertraute Domäne beim Herstellen einer Verbindung zu Intune und beim Verwenden von Ressourcen.
4	Hinzufügen von Benutzern und Gruppen: Fügen Sie Benutzer und Gruppen hinzu, oder verbinden Sie Active Directory Domain Services für die Synchronisierung mit Intune. Dies ist erforderlich, es sei denn, Ihre Geräte sind „benutzerlose“ Kiosk-Geräte. Gruppen werden verwendet, um Apps, Einstellungen und andere Ressourcen zuzuweisen.
5	Zuweisen von Lizenzen: Erteilen Sie Benutzern die Berechtigung, Intune zu verwenden. Jeder Benutzer oder jedes benutzerlose Gerät benötigt eine Lizenz für Intune, um auf den Dienst zuzugreifen.
6	Festlegen der MDM-Autorität: Verwenden Sie Benutzer- und Gerätegruppen, um Verwaltungsaufgaben zu vereinfachen. Gruppen werden verwendet, um Apps, Einstellungen und andere Ressourcen zuzuweisen.
7	Hinzufügen von Apps: Apps können Gruppen zugewiesen und automatisch oder optional installiert werden.
8	Konfigurieren von Geräten: Richten Sie Profile ein, die Einstellungen für Geräte verwalten. Mit Geräteprofilen können Einstellungen für E-Mail-, VPN-, WLAN- und Gerätefunktionen vorkonfiguriert werden. Sie können auch Geräte zum Schutz von Geräten und Daten einschränken.

9	Anpassen des Unternehmensportals: Passen Sie das Intune-Unternehmensportal an, mit dem Benutzer Geräte registrieren und Apps installieren. Diese Einstellungen werden in der Unternehmensportal-App und auf der Intune-Unternehmensportal-Website angezeigt.
10	Aktivieren der Geräteregistrierung: Aktivieren Sie die Intune-Verwaltung auf iOS/iPadOS-, Windows-, Android- und Mac-Geräten, indem Sie die MDM-Autorität festlegen und bestimmte Plattformen aktivieren.
11	Konfigurieren der App-Richtlinien: Legen Sie bestimmte Einstellungen anhand der App-Schutzrichtlinien in Microsoft Intune fest.

Die wichtigsten Szenarien werden auf den kommenden Seiten kurz vorgestellt.

Dokumentbeginn

Mobile Device Management

Intune ermöglicht es Ihnen, die Geräte und Apps Ihrer Mitarbeiter sowie deren Zugriff auf Unternehmensdaten zu verwalten. Damit diese mobile Geräteverwaltung (Mobile Device Management, MDM) genutzt werden kann, müssen die Geräte zunächst beim Intune-Dienst registriert werden. Wenn ein Gerät registriert ist, wird ein MDM-Zertifikat für das Gerät ausgestellt. Dieses Zertifikat wird für die Kommunikation mit dem Intune-Dienst verwendet.

Zu BYOD-Geräten (Bring Your Own Device) gehören Mobiltelefone, Tablets und PCs, die persönliches Eigentum der Benutzer sind. Benutzer installieren die Unternehmensportal-App und führen diese zur Registrierung ihrer Geräte aus. Dieses Programm ermöglicht Benutzern den Zugriff auf Unternehmensressourcen wie E-Mails.

Unternehmenseigene Geräte (Corporate-Owned Devices, COD) umfassen Mobiltelefone, Tablets und PCs, die das Eigentum der Organisation sind und an die Mitarbeiter ausgegeben werden. Die Registrierung von COD-Geräten unterstützt Szenarien wie die automatische Registrierung, freigegebene Geräte oder Anforderungen für eine vorab autorisierte Registrierung. Eine Methode zum Registrieren von COD-Geräten besteht darin, dass ein Administrator oder Vorgesetzter den Geräteregistrierungs-Manager verwendet. iOS-/iPadOS-Geräte können direkt über die von Apple bereitgestellten ADE-Tools registriert werden. Geräte mit einer IMEI-Nummer können auch als unternehmenseigene Geräte identifiziert und gekennzeichnet werden.

Wie hinter diesem Link beschrieben, gibt es verschiedene Methoden, um die Geräte Ihrer Mitarbeiter zu registrieren. Die einzelnen Methoden hängen vom Gerätebesitz (persönlich oder unternehmenseigen), vom Gerätetyp (iOS, Windows, Android) und den Verwaltungsanforderungen (Zurücksetzungen, Affinität, Sperren) ab.

Mehr erfahren Sie hier:

- Intune-Registrierungsmethoden für Windows-Geräte
- Registrieren von Android-Geräten
- Registrieren von iOS-/iPadOS-Geräten in Intune

Dokumentbeginn

Autopilot

Windows Autopilot vereinfacht das Registrieren von Geräten. Mit Microsoft Intune und Autopilot können Sie Ihren Endbenutzern neue Geräte geben, ohne die benutzerdefinierten Betriebssystemimages erstellen, verwalten und auf diese anwenden zu müssen.

In diesem Abschnitt finden Sie Folgendes:

- Hinzufügen von Geräten zu Intune
- Erstellen einer Autopilot-Gerätegruppe
- Erstellen eines Autopilot-Bereitstellungsprofils
- Zuweisen des Autopilot-Bereitstellungsprofils zur Gerätegruppe
- Verteilen von Windows-Geräten an Benutzer

Wenn Sie über kein Intune-Abonnement verfügen, registrieren Sie sich für eine kostenlose Testversion.

Eine Übersicht über die Vorteile, Szenarien und Voraussetzungen von Autopilot finden Sie unter Übersicht über Windows Autopilot.

Voraussetzungen

- Schnellstart: Einrichten der automatischen Registrierung für Windows 10-Geräte
- Azure Active Directory Premium-Abonnement

Hinzufügen von Geräten

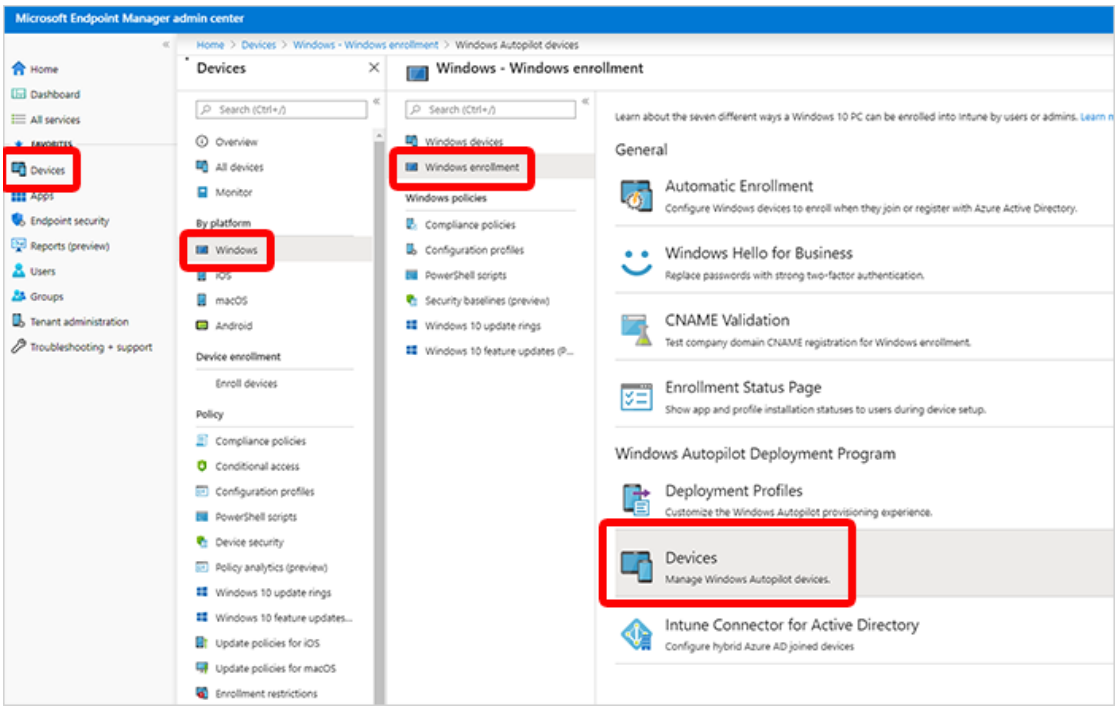
Der erste Schritt beim Einrichten von Windows Autopilot besteht darin, die Windows-Geräte zu Intune hinzuzufügen. Sie müssen lediglich eine CSV-Datei erstellen und in Intune importieren.

1. Erstellen Sie in einem beliebigen Text-Editor eine CSV-Datei (Comma-Separated Values), die die Windows-Geräte identifiziert. Verwenden Sie das folgende Format:

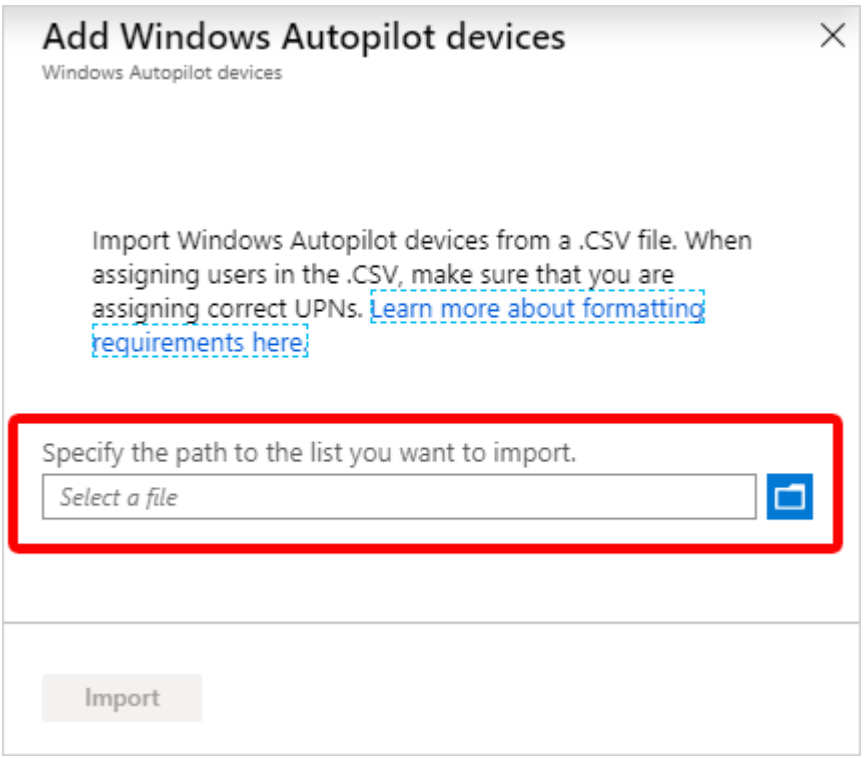
   Seriennummer, *Windows-Produkt-ID*, *Hardwarehash*, *Optionales Gruppentag*

   Die ersten drei Elemente sind erforderlich, das Gruppentag (früher „Auftrags-ID") hingegen ist optional.

2. Speichern Sie die CSV-Datei.
3. Klicken Sie im Microsoft Endpoint Manager Admin Center auf G**eräte → Windows → Geräte** (unter „**Windows Autopilot Deployment-Programm**" → **Importieren).**



4. Navigieren Sie unter „**Windows Autopilot-Geräte hinzufügen“** zu der CSV-Datei, die Sie gespeichert haben.



5. Wählen Sie „**Importieren“** aus, um mit dem Importieren von Informationen zu den Geräten zu beginnen. Der Import kann mehrere Minuten dauern.
6. Klicken Sie nach Abschluss des Imports unter „Windows Autopilot Deployment-Programm“ → Synchronisieren auf „Geräte“ → Windows → Windows-Registrierung →

Geräte. Eine Meldung zeigt an, dass die Synchronisierung ausgeführt wird. Der Prozess kann ein paar Minuten in Anspruch nehmen, je nachdem, wie viele Geräte Sie synchronisieren.

7. Aktualisieren Sie die Ansicht, um neue Geräte anzuzeigen.

Erstellen einer Autopilot-Gerätegruppe

Als Nächstes erstellen Sie eine Gerätegruppe und platzieren darin die Autopilot-Geräte, die Sie gerade geladen haben.

1. Klicken Sie im Microsoft Endpoint Manager Admin Center auf die Option **Gruppen → Neue Gruppe**.
2. Auf der Seite „**Gruppe“**:
   - Wählen Sie für „**Gruppentyp“** die Option „**Sicherheit“**.
   - Geben Sie für „**Gruppenname**“ *Autopilot-Gruppe* ein. Geben Sie für „**Gruppenbeschreibung“** *Testgruppe für Autopilot-Geräte* ein.
   - Wählen Sie für „**Mitgliedschaftstyp“ die Option „Zugewiesen“** aus.
3. Wählen Sie auf der Seite „**Gruppe“ die Option „Mitglieder**“ aus, und fügen Sie die Autopilot-Geräte der Gruppe hinzu. Autopilot-Geräte, die noch nicht registriert sind, sind Geräte, deren Name der Seriennummer des Geräts entspricht.
4. Wählen Sie „**Erstellen“** aus.

Erstellen eines Autopilot-Bereitstellungsprofils

Nach dem Erstellen einer Gerätegruppe müssen Sie ein Bereitstellungsprofil erstellen, um die Autopilot-Geräte konfigurieren zu können.

1. Klicken Sie im Microsoft Endpoint Manager Admin Center auf **Geräte → Windows → Windows-Registrierung → Deployment Profiles** („Bereitstellungsprofile“) **→ Profil erstellen.**
2. Geben Sie auf der Seite „**Grundlagen“** als „Name“ *Autopilot-Profil* ein. Geben Sie für „**Beschreibung“** *Testprofil für Autopilot-Geräte* ein.
3. Legen Sie „**Alle als Ziel angegebenen Geräte in Autopilot konvertieren“** auf „Ja“ fest. Durch diese Einstellung wird sichergestellt, dass alle Geräte in der Liste beim Autopilot-Bereitstellungsdienst registriert werden. Die Verarbeitung der Registrierung kann 48 Stunden dauern.
4. Wählen Sie „Weiter“ aus.
5. Wählen Sie auf der Seite „**Out-of-Box-Experience (OOBE)“** als „**Bereitstellungsmodus“ die Option „Benutzergesteuert“** aus. Geräte mit diesem Profil werden dem Benutzer zugeordnet, der das Gerät registriert. Für die Registrierung des Geräts sind Benutzeranmeldeinformationen erforderlich.
6. Wählen Sie im Feld „**Verknüpfen mit Azure AD als“** die Option „**In Azure AD eingebunden“**.

7. Konfigurieren Sie die folgenden Optionen, und übernehmen Sie für die anderen die Standardwerte:
    - **Microsoft-Software-Lizenzbedingungen: Ausblenden**
    - **Datenschutzeinstellungen: Anzeigen**
    - **Art des Benutzerkontos: Standard**
8. Wählen Sie „**Weiter**“ aus.
9. Wählen Sie auf der Seite „**Zuweisungen“** für „**Zuweisen an“** die Option „**Ausgewählte Gruppen**“ aus.
10. Wählen Sie „**Wählen Sie die Gruppen aus, die eingeschlossen werden sollen“** und dann „**Autopilot-Gruppe“** aus.
11. Wählen Sie „**Weiter**“ aus.
12. Wählen Sie auf der Seite „**Überprüfen + Erstellen**“ den Befehl „**Erstellen**“ aus, um das Profil zu erstellen.

Verteilen von Geräten an Benutzer

Sie können nun die Windows-Geräte an Ihre Benutzer verteilen. Wenn sie sich zum ersten Mal anmelden, registriert und konfiguriert das Autopilot-System automatisch die Geräte.

Bereinigen der Ressourcen

Wenn Sie die Autopilot-Geräte nicht mehr verwenden möchten, können Sie sie löschen.

1. Wenn Geräte bei Intune registriert sind, müssen Sie sie zunächst aus dem Azure Active Directory-Portal löschen.
2. Klicken Sie im Microsoft Endpoint Manager Admin Center auf G**eräte → Windows → Windows-Registrierung → Geräte** (unter „**Windows Autopilot Deployment-Programm**“**).**
3. Wählen Sie die Geräte aus, die Sie löschen möchten, und klicken Sie dann auf „**Löschen**“.
4. Bestätigen Sie den Löschvorgang mit „Ja“. Der Löschvorgang kann einige Minuten dauern.

Dokumentbeginn

Mobile Application Management (MAM)

Als IT-Administrator können Sie mit Microsoft Intune die Client-Apps verwalten, die Mitarbeiter Ihres Unternehmens verwenden. Diese Funktion besteht zusätzlich zur Verwaltung von Geräten und dem Schutz von Daten. Eine der Prioritäten eines Administrators ist es, sicherzustellen, dass die Endbenutzer Zugriff auf die Apps haben, die sie für ihre Arbeit benötigen. Dieses Ziel kann aus verschiedenen Gründen eine große Herausforderung darstellen:

- Es gibt eine Vielzahl von Geräteplattformen und App-Typen.
- Sie müssen möglicherweise Apps auf unternehmenseigenen und auf privaten Geräten verwalten.
- Sie müssen sicherstellen, dass Ihr Netzwerk und Ihre Daten weiterhin geschützt sind.

Darüber hinaus sollten Sie Apps auf Geräten, die nicht bei Intune registriert sind, zuweisen und verwalten.

Die mobile Anwendungsverwaltung (Mobile Application Management, MAM) von Intune bezeichnet die Intune-Verwaltungsfunktionen, mit denen Sie mobile Apps für Ihre Benutzer veröffentlichen, per Push bereitstellen, konfigurieren, schützen, überwachen und aktualisieren.

MAM ermöglicht es Ihnen, die Daten Ihres Unternehmens innerhalb einer Anwendung zu verwalten und zu schützen. Mit **MAM ohne Geräteregistrierung** (MAM-WE) kann eine Geschäfts-, Schul- oder Uni-App, die vertrauliche Daten enthält, auf nahezu jedem Gerät verwaltet werden, auch auf persönlichen Geräten in **BYOD-Szenarien (Bring Your Own Device)**. Viele Produktivitäts-Apps, wie zum Beispiel die Microsoft Office-Apps, können über Intune MAM verwaltet werden. Weitere Informationen finden Sie in der Liste von in Microsoft Intune verwalteten Apps, die für die Öffentlichkeit verfügbar ist.

Intune MAM unterstützt zwei Konfigurationen:

- **Intune MDM und MAM**: IT-Administratoren können Apps mithilfe von MAM und App-Schutzrichtlinien nur auf Geräten verwalten, die bei der Intune-Verwaltung mobiler Geräte (Mobile Device Management, MDM) registriert sind. Um Apps mithilfe von MDM und MAM zu verwalten, sollten Kunden die Intune-Konsole im Azure Portal unter https://portal.azure.com verwenden.
- **MAM ohne Geräteregistrierung**: Mit MAM ohne Geräteregistrierung (MAM without Enrollment, MAM-WE) können IT-Administratoren Apps mithilfe von MAM und App-Schutzrichtlinien auf Geräten verwalten, die nicht bei Intune MDM registriert sind. Dies bedeutet, dass Apps über Intune auf Geräten verwaltet werden können, die bei EMM-Drittanbietern (Enterprise Mobility Management, EMM) registriert sind. Um Apps mithilfe von MAM-WE zu verwalten, sollten Kunden unter https://portal.azure.com die Intune-Konsole im Azure Portal verwenden. Darüber hinaus können Apps auf Geräten, die entweder bei EMM-Drittanbietern oder überhaupt nicht bei einer MDM-Lösung registriert sind, von Intune verwaltet werden. Weitere Informationen über BYOD und EMS von Microsoft finden Sie unter Technologieentscheidungen zur Ermöglichung von BYOD mit Microsoft Enterprise Mobility + Security (EMS).

Weiterführende Links:

- Schnellstart: Hinzufügen und Zuweisen einer Client-App
- Schnellstart: Erstellen und Zuweisen einer App-Schutzrichtlinie

Dokumentbeginn

VPN Split-Tunneling

Wenn die Anzahl der Remote- bzw. Homeoffice-Mitarbeiter ansteigt, kann dies zu Lasten des VPN-Gateways gehen. Im schlimmsten Fall bildet das VPN-Gateway sogar einen Flaschenhals und es kommt zu Netzwerkunterbrechungen oder sehr hohen Latenzzeiten, die das Arbeiten unnötig erschweren. Aus diesem Grund empfiehlt Microsoft die Nutzung von Microsoft Teams, SharePoint Online und Exchange Online mithilfe eines Split-Tunnelings. Dies bedeutet, dass die netzwerk- und lastintensiven Verbindungen der genannten Services nicht über das VPN Gateway geleitet werden, sondern eine direkte Verbindung zur Office 365 Cloud aufbauen dürfen.

Die Verbindungen zwischen Office 365 und dem Client sind dabei stets verschlüsselt. Im folgenden Schaubild sehen Sie eine mögliche Architektur für Split-Tunneling. Eine Übersicht aller fünf möglichen Szenarien finden Sie hier: https://docs.microsoft.com/en-us/office365/enterprise/office-365-vpn-implement-split-tunnel#common-vpn-scenarios

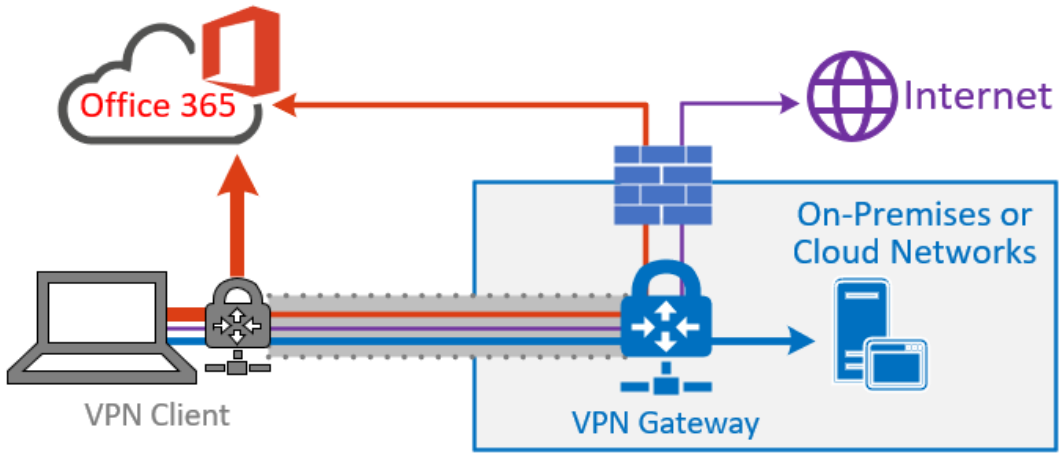


Abbildung 22: Darstellung der Nutzung von VPN Split-Tunneling

IP-Adressen und URLs

Um das Split-Tunneling zu konfigurieren, ist es wichtig zu wissen, welche IP-Adressen und URLs nicht über das VPN-Gateway geleitet werden müssen. Microsoft teilt alle verwendeten URLs und IP-Adressen in drei Kategorien ein, wobei nur die Kategorie „Optimize" im Split-Tunneling konfiguriert werden muss. Die Kategorien „Allow" und „Default" sind für dieses Szenario zweitrangig.

Tabelle 5: URLs samt Ports für die Nutzung im Split-Tunneling

Optimize-URLs	**Port/Protocol**
https://outlook.office365.com	TCP 443
https://outlook.office.com	TCP 443
https://<tenant.sharepoint.com	TCP 443
https://<tenant-my.sharepoint.com	TCP 443
Teams Media IPs (keine URL)	UDP 3478, 3479, 3480 und 3481

Insbesondere für die IP-Adressen wird empfohlen, Skripte zu verwenden, weil diese sich ändern können und dadurch zu erhöhten administrativen Aufwänden führen.

Tabelle 6: Optimize-IP-Adressbereiche

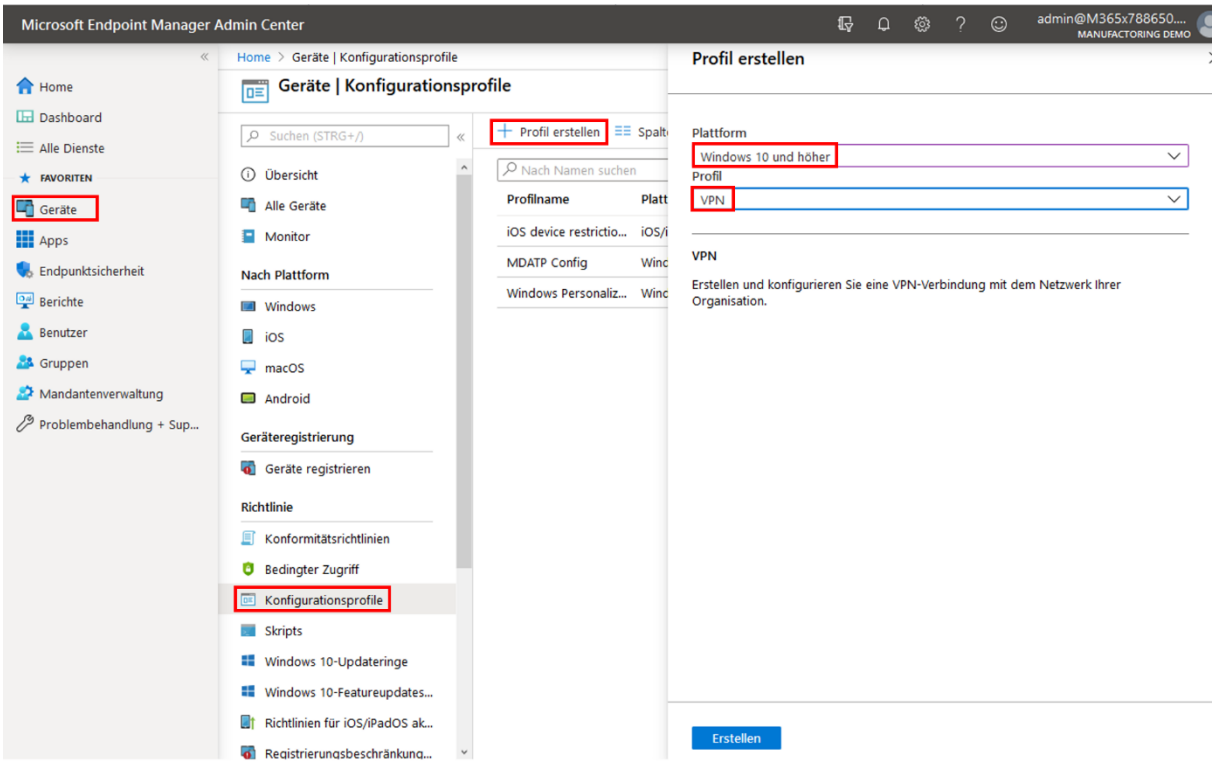
104.146.128.0/17	191.234.140.0/22
13.107.128.0/22	204.79.197.215/32
13.107.136.0/22	23.103.160.0/20
13.107.18.10/31	40.104.0.0/15
13.107.6.152/31	40.108.128.0/17
13.107.64.0/18	40.96.0.0/13
131.253.33.215/32	52.104.0.0/14
132.245.0.0/16	52.112.0.0/14
150.171.32.0/22	52.96.0.0/14
150.171.40.0/22	52.120.0.0/14

Eine Liste aller URLs und IP-Adressen für alle drei Kategorien finden Sie hier: https://docs.microsoft.com/de-de/office365/enterprise/urls-and-ip-address-ranges

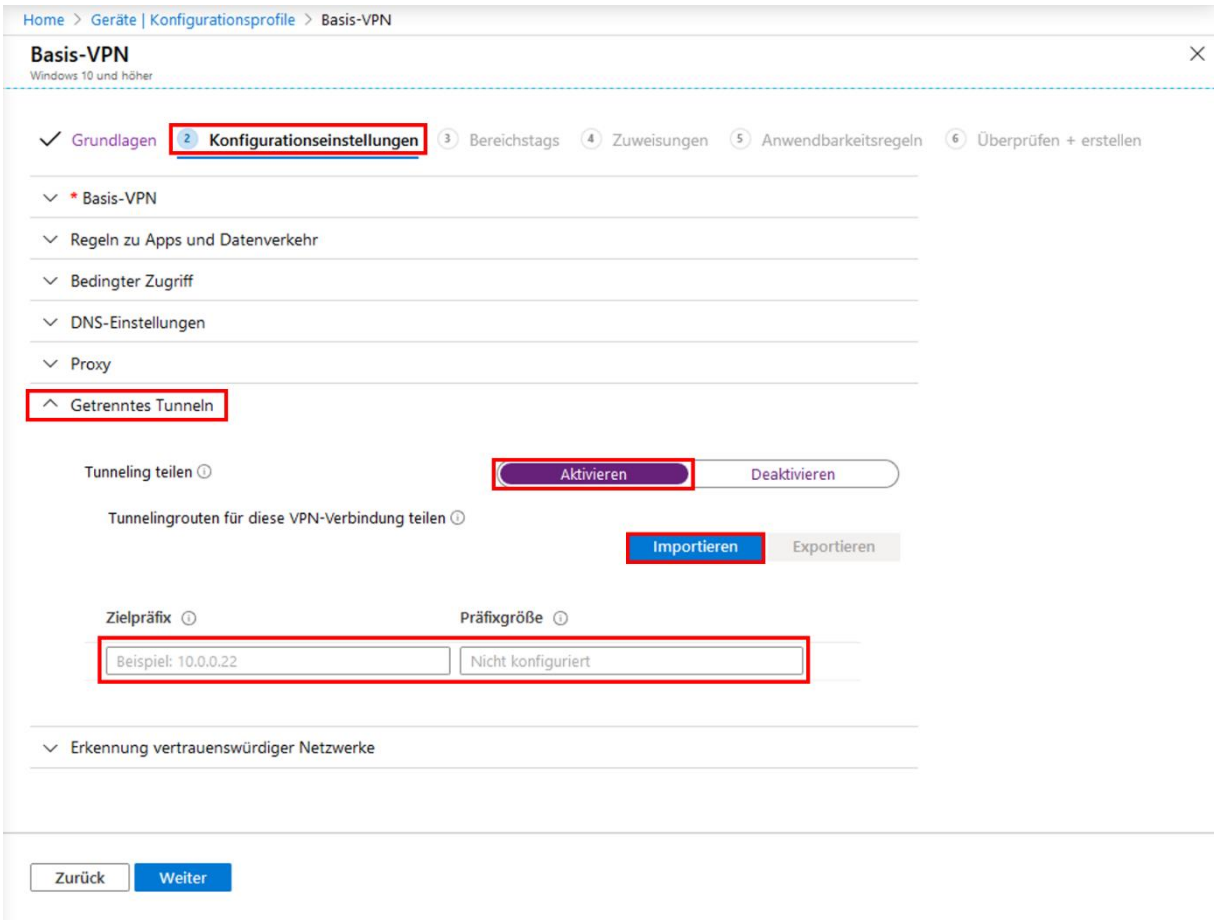
Konfiguration mit Microsoft Endpoint Manager (ehem. Intune)

Die Konfiguration des Split-Tunneling VPN ist abhängig von Ihrem VPN-Client. Trotzdem können viele verschiedene Anbieter auch im Microsoft Endpoint Manager für Windows 10, MacOS und iOS konfiguriert werden.

Öffnen Sie den Microsoft Endpoint Manager, klicken Sie auf Geräte → Konfigurationsprofile → „Profil erstellen“ und wählen Sie die gewünschte Plattform sowie das Profil „VPN“.



Im Konfigurationsprofil selbst haben Sie unter „2 Konfigurationseinstellungen“ die Option „Getrenntes Tunneln“ (oder Split-Tunneling), wo Sie per CSV-Import oder manueller Eingabe die oben genannten IP-Adressen angeben.



Die Konfigurationsmöglichkeiten variieren je nach Betriebssystem und VPN-Lösung.

Eine Auswahl von Leitfäden zur Optimierung des Office 365-Datenverkehrs finden Sie hier:

- **Cisco AnyConnect**: Optimieren des AnyConnect-Split-Tunnels für Office365
- **Palo Alto GlobalProtect**: Optimieren des Office 365-Datenverkehrs über einen geteilten VPN-Tunnel mit Zugriffsausschlussroute
- **F5 Networks BIG-IP APM**: Optimieren des Office 365-Datenverkehrs beim Remotezugriff über VPNs bei Verwendung von BIG-IP APM

Dokumentbeginn

Datenschutz, Privatsphäre und DSGVO

- Blogpost „Datenschutz bei Microsoft“
- Blogpost „Increased Transparency and Control over data“
- Blogpost „Our Commitment to GDPR“
- Corporate Responsibility beim Datenschutz
- Office 365-Daten in neuen Rechenzentren in Deutschland
- Wo wir Ihre Daten speichern
- Microsoft Trust Center
- Microsoft Service Trust Portal
- Microsoft Audit-Berichte, zum Beispiel ISO27001 und DSGVO
- Microsoft Online Service Terms
- Microsoft Data Privacy Addendum
- Content Removal Request Report
- Microsoft Account Privacy Settings
- Microsoft-Zertifizierungen für die Cloud

Mitbestimmung beim Einsatz von Clouddiensten
Eine umfangreiche Darstellung der Herangehensweise an das Thema Mitbestimmung finden Sie in folgendem Sway: https://sway.office.com/NnD7zky8kfVik0wG?ref=Link

Auch dieses Thema eignet sich nicht für eine verkürzte Darstellung im Rahmen dieses Guides.

Dokumentbeginn

Weitere Informationen

Weitere Dokumentation zu Sicherheits- und Verwaltungsfunktionen für Remotemitarbeiter:
https://docs.microsoft.com/de-de/enterprise-mobility-security/remote-work/

Unterstützung von Microsoft für Kunden und Partner in Zeiten von COVID-19:
https://news.microsoft.com/de-de/features/alle-infos-zu-covid-19-so-unterstuetzt-microsoft/

Microsoft Deutschland-Startseite für das Thema „Sicherheit im Enterprise-Umfeld“:
https://www.microsoft.com/de-de/security/business

Dokumentbeginn


Microsoft