Microsoft 365

Das umfassende Handbuch

DIE LESEPROBE

Kapitel 4

Identitäten und Active Directory-Synchronisierung

In diesem Kapitel lernen Sie verschiedene Identitätsarten kennen, richten Single Sign-on ein und koppeln in verschiedenen Varianten Ihr lokales Active Directory mit Entra ID.

Ihr Microsoft 365-Mandant verfügt mit *Entra ID* (früher wurde der Name *Azure Active Directory (AAD)* verwendet) über einen eigenen Verzeichnisdienst. Entra ID bildet die Grundlage für alle Microsoft 365-Dienste, und für jeden Anwender müssen Sie dort ein Benutzerkonto anlegen und lizenzieren. Typischerweise betreiben Sie aber bereits lokal ein Active Directory, und damit stellt sich die Frage, wie Sie diese beiden Verzeichnisse miteinander integrieren, sodass Sie von administrativer Seite keinen zusätzlichen Aufwand und ihre Anwender keine Schwierigkeiten beim Anmelden haben. In den meisten Fällen installieren Sie dazu auf einem lokalen Server eine Softwarekomponente, die in regelmäßigen Abständen insbesondere lokal vorhandene Benutzerkonten, Gruppen und Kontakte automatisch im Verzeichnisdienst von Microsoft 365 anlegt und Änderungen an diesen Objekten überträgt. Dadurch entfällt für Sie als Administrator der doppelte Pflegeaufwand, beispielsweise beim Anlegen von Benutzerkonten für neue Mitarbeiter.

In diesem Kapitel lernen Sie unterschiedliche Integrationsvarianten der beiden Verzeichnisdienste mit ihren Vor- und Nachteilen kennen. Darunter sind auch Verfahren, die ein Single Sign-on bereitstellen, um die Anmeldung Ihren Anwendern besonders einfach zu machen.

4.1 Verschiedene Identitäten

Microsoft 365 verwendet intern mit *Entra ID* einen eigenen Verzeichnisdienst, so wie Sie selbst höchstwahrscheinlich lokal ein Active Directory einsetzen. Für jeden Ihrer Microsoft 365-Anwender muss in Entra ID ein Benutzerkonto angelegt sein, das dann für die verschiedenen Dienste lizenziert wird (siehe Abbildung 4.1).

Die Benutzerkonten in Entra ID werden aus Sichtweise der Administration *Microsoft-Online-IDs* genannt. Bei Endanwendern werden dagegen die Begriffe *Organisations-*, *Geschäfts-*, *Schul-* und *Uni-Konto* angewendet. Diese Begriffe finden sich bei verschiedenen Anmeldedialogen, wie beispielsweise in Abbildung 4.2.

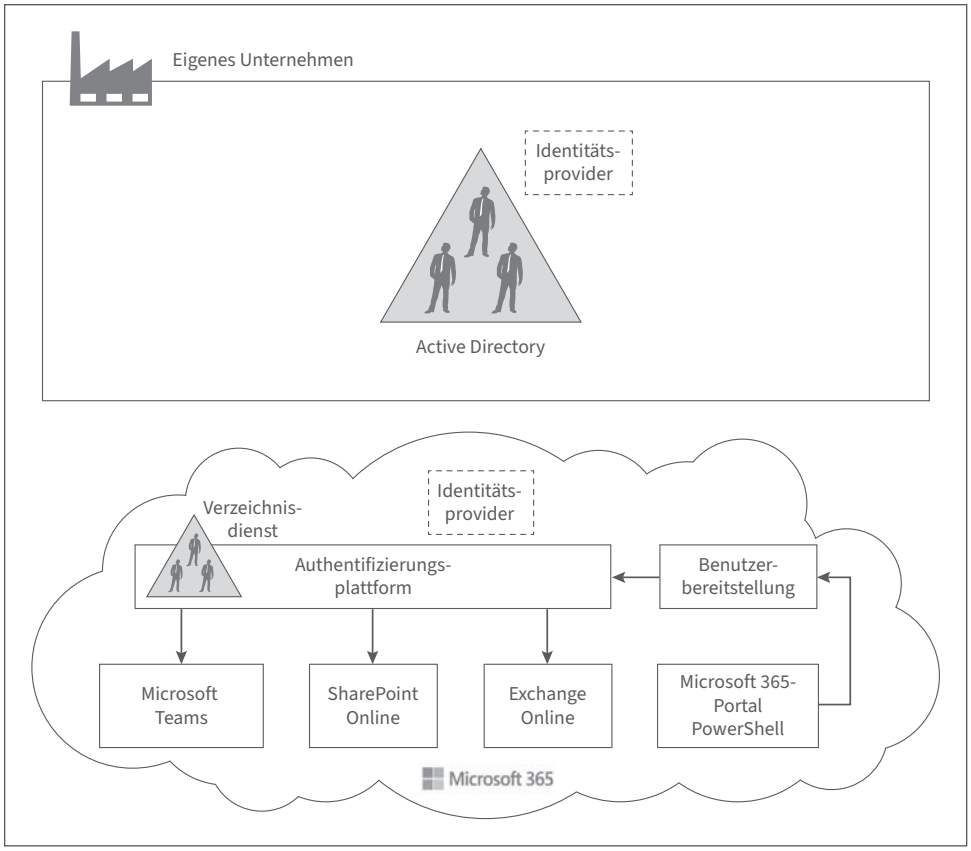

Abbildung 4.1: Microsoft 365 verfügt über einen eigenen Verzeichnisdienst.

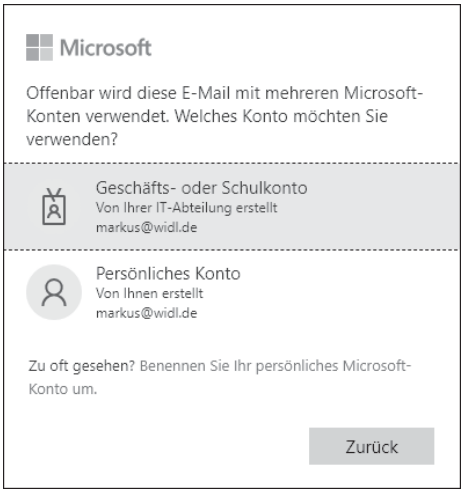

Abbildung 4.2: Anmeldedialog

Gemeint ist dabei immer ein Benutzerkonto in einem beliebigen Entra ID-Verzeichnis. Ein *Microsoft-Konto* (auch bekannt unter dem englischen Begriff *Microsoft Account* mit der Abkürzung *MSA* oder früher auch *Live ID* genannt) oder *Persönliches Konto* ist übrigens keine Microsoft-Online-ID, denn es kommt dabei ein separater Verzeichnisdienst zum Einsatz.

Entra ID wird in verschiedenen Ausbaustufen über verschiedene Lizenztypen angeboten. In jeder Lizenzvariante von Microsoft 365 enthalten ist mindestens die Free-Edition. Für die meisten in diesem Kapitel beschriebenen Funktionen ist die Free-Edition ausreichend, allerdings gibt es auch Ausnahmen, auf die ich jeweils besonders hinweise. Insbesondere Funktionen aus dem Sicherheitsbereich erfordern Lizenzen vom Typ *Entra ID P1* oder *P2*. Diese sind in den folgenden Lizenzpaketen aus Tabelle 4.1 bereits enthalten, können jedoch auch einzeln erworben werden.

Entra ID-Lizenztyp	Enthalten in diesen Paketen
Entra ID P1	Microsoft 365 E3 EMS E3
Entra ID P2	Microsoft 365 E7 Microsoft 365 E5 EMS E5

Tabelle 4.1: Entra ID-Lizenzen

Mehr zu Entra ID finden Sie hier:

www.microsoft.com/de-de/security/business/microsoft-entra-pricing

Entra ID wird übrigens nicht nur von Microsoft 365, sondern beispielsweise auch von anderen Diensten wie *Dynamics 365* eingesetzt. So können all diese Dienste auf ein gemeinsames Entra ID-Verzeichnis zugreifen – und Sie sparen sich die Administration weiterer Verzeichnisse.

Die Frage ist nun, wie Sie in der Praxis mit diesem zusätzlichen Verzeichnisdienst umgehen, da Sie ja normalerweise bereits mit dem Active Directory über einen solchen verfügen. Dabei gibt es mehrere verschiedene Szenarien, ob und wie Sie ein vorhandenes Active Directory mit Entra ID anbinden.

4.2 Szenarien zur Active Directory-Integration

Um die möglichen Szenarien zu verstehen, müssen wir zunächst die Bedeutung einer Reihe von Komponenten klären, aus denen Sie für Ihr Unternehmen die geeignete Strategie für den Umgang mit Identitäten zusammensetzen.

4.2.1 Verzeichnissynchronisierung

Mit der Einrichtung der Verzeichnissynchronisierung koppeln Sie das lokal vorhandene Active Directory mit Entra ID aus Microsoft 365. Die Synchronisierung erspart Ihnen von administrativer Seite viel Verwaltungsaufwand, denn Objekte, die Sie beispielsweise bereits im Active Directory angelegt haben, müssen Sie nicht erneut in Entra ID anlegen und pflegen. Dazu werden in einem regelmäßigen Intervall Objekte des einen Verzeichnisses im anderen nachgepflegt. Das betrifft sowohl das Anlegen von Objekten als auch ihre Änderung oder ihre Löschung. So werden beispielsweise die Active Directory-Benutzer in Entra ID von Microsoft 365 automatisch angelegt, und Sie müssen sie nur noch mit einer Lizenz (und gegebenenfalls einem Kennwort) ausstatten. Grundsätzlich erfolgt dabei die Synchronisierung vom lokalen Active Directory aus zu Entra ID. Wir werden jedoch auch Szenarien besprechen, bei denen aus Entra ID ins lokale Active Directory synchronisiert wird.

Rein funktional handelt es sich bei Entra ID nicht einfach um einen Windows-Domänencontroller in der Cloud. Entra ID verfügt über Funktionen, die im lokalen Active Directory nicht zur Verfügung stehen, beispielsweise über die mehrstufige Authentifizierung. Dagegen gibt es im Active Directory Funktionalitäten, beispielsweise Gruppenrichtlinien, die es Entra ID so nicht gibt. Sehen Sie Entra ID als funktionale Erweiterung Ihres bestehenden Active Directorys an.

Die Verzeichnissynchronisierung selbst können Sie über verschiedene Wege umsetzen:

- *Entra Connect*

  Diese Variante ist die historisch ältere und, zumindest heute noch, die funktional leistungsfähigere. Hier installieren Sie im lokalen Netzwerk die Software *Entra Connect*, die die Objekte zwischen Active Directory und Entra ID synchronisiert.

  Mit Entra Connect sind sehr vielfältige Anpassungsmöglichkeiten vorhanden, doch gestalten sie sich in der Praxis als durchaus komplex. Auch benötigt Entra Connect einen lokalen SQL Server. In kleineren Umgebungen (abhängig von der Anzahl der zu synchronisierenden Objekte) kann die kostenfreie Variante *Microsoft SQL Server Express LocalDB* zum Einsatz kommen. In größeren Umgebungen ist dagegen ein ausgewachsener (und separat zu lizenzierender) SQL Server erforderlich. Bestimmte Szenarien sind auch nur mit Entra Connect abbildbar. Zu diesen Szenarien zählt die Exchange-Hybridbereitstellung, bei der Sie neben einer lokalen Exchange-Umgebung Exchange Online parallel betreiben (siehe Abschnitt 6.10, »Vollständige Exchange-Hybridkonfiguration«). Abbildung 4.3 zeigt den grundsätzlichen Aufbau.

- *Entra Cloud Sync*

  Auch wenn der Name auf eine gewisse Ähnlichkeit hindeutet, ist der Aufbau doch sehr unterschiedlich. Zwar müssen Sie auch hier lokal eine Softwarekomponente installieren, doch handelt es sich bei ihr nur um einen recht einfach gehaltenen Agenten, der als Kommunikationsbrücke zwischen dem Active Directory und Entra ID fungiert. Die eigentliche Synchronisierungslogik läuft hier nicht lokal, sondern in der Cloud (daher rührt wohl auch der Name Cloud Sync).

  Der lokal zu installierende Agent ist dabei recht einfach gehalten. Ein SQL Server ist für seinen Betrieb auch nicht erforderlich. In Abbildung 4.4 sehen Sie den grundsätzlichen Aufbau.

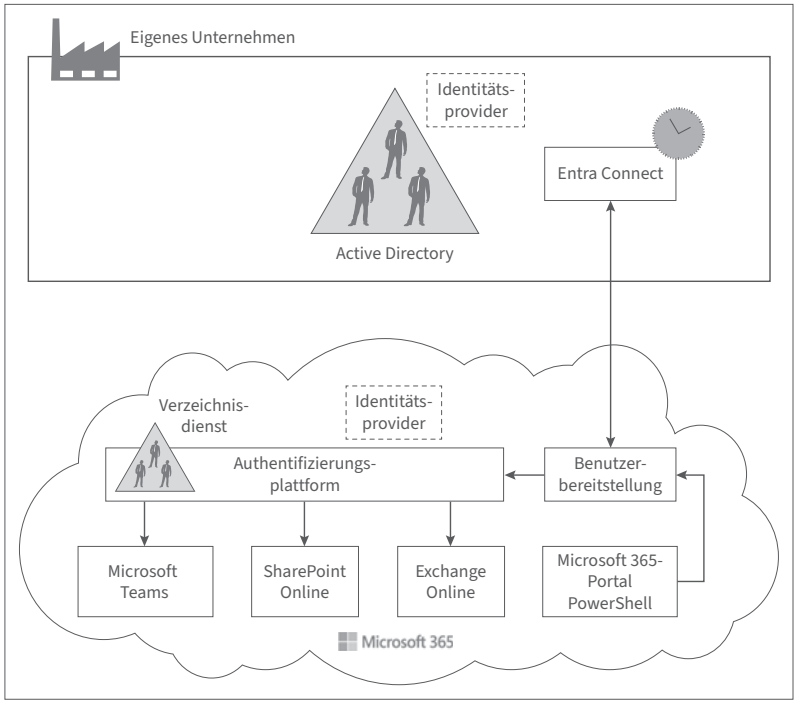

Abbildung 4.3: Verzeichnissynchronisierung mit Entra Connect

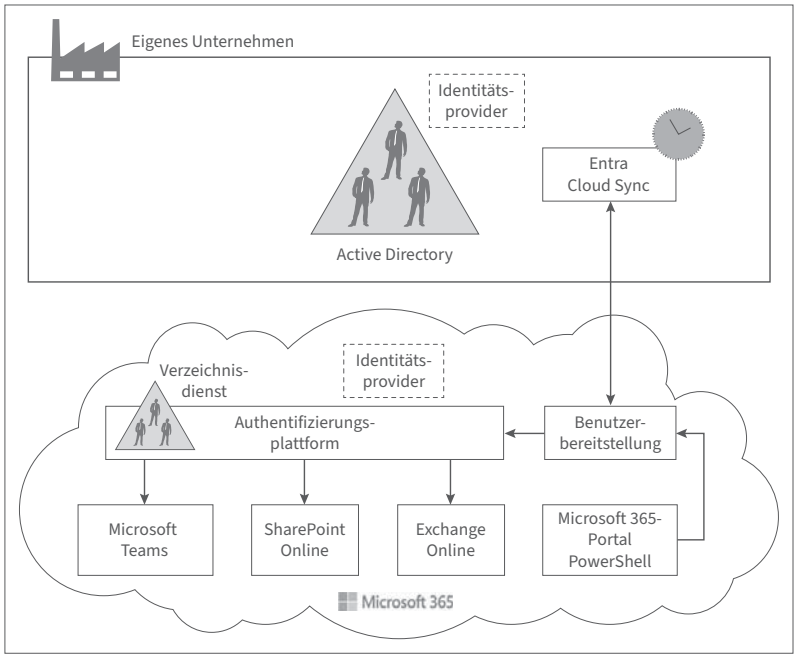

Abbildung 4.4: Verzeichnissynchronisierung mit Entra Cloud Sync

In Tabelle 4.2 finden Sie die wichtigsten Unterscheidungsmerkmale zwischen Entra Connect und Entra Cloud Sync, um Ihnen die Entscheidung für die eine oder andere Variante zu vereinfachen.

Merkmal	Entra Connect	Entra Cloud Sync
Verbindung mit einem einzelnen AD Forest	ja	ja
Verbindung mit mehreren AD Forests	ja	ja
Verbindung mit mehreren getrennten AD Forests	nein	ja
Konfiguration der Synchronisierung	lokal	Cloud
lokaler SQL Server (ggf. Microsoft SQL Server Express LocalDB) erforderlich	ja	nein
Objektsynchronisation	Benutzer, Gruppen, Kontakte, Geräte	Benutzer, Gruppen, Kontakte
Synchronisierung der Attribute `extensionAttribute1` … `15`	ja	ja
Synchronisierung eigener AD-Attribute	ja	nein
Unterstützt Exchange-Hybridbereitstellung (siehe Abschnitt 6.10, »Vollständige Exchange-Hybridkonfiguration«).	ja	nein
Unterstützt Kennwort-Hashsynchronisierung.	ja	ja
Unterstützt Passthrough-Authentifizierung (siehe Abschnitt 4.2.3, »Passthrough-Authentifizierung (PTA)«).	ja	nein
Unterstützt Single Sign-on (siehe Abschnitt 4.2.4, »Single Sign-on«).	ja	ja
Unterstützt Identitätsverbund (siehe Abschnitt 4.5, »Identitätsverbund«).	ja	ja
Unterstützt das Kennwortrückschreiben (siehe Abschnitt 4.3.4, »Installation und Konfiguration«).	ja	ja
Unterstützt das Geräterückschreiben (siehe Abschnitt 4.3.4, »Installation und Konfiguration«).	ja	nein
Unterstützt das Gruppenrückschreiben (siehe Abschnitt 4.3.4, »Installation und Konfiguration«).	ja	nein

Tabelle 4.2: Vergleich von Entra Connect und Entra Cloud Sync

Merkmal	Entra Connect	Entra Cloud Sync
Unterstützt die Installation auf einem Domänencontroller.	ja	ja
Filterung der zu synchronisierenden Domänen, Organisationseinheiten und Gruppen	ja	ja
Filterung der zu synchronisierenden Objekte nach eigenen Abfrageregeln	ja	nein

Tabelle 4.2: Vergleich von Entra Connect und Entra Cloud Sync (Forts.)

- *Microsoft Identity Manager (MIM)* und *EMCA Host Connector*

  Da diese beiden Varianten nur für spezielle Szenarien gedacht sind, berücksichtige ich sie in diesem Buch nicht weiter. Sollten Sie dazu Informationen benötigen, finden Sie sie auf folgender Webseite: *https://learn.microsoft.com/de-de/entra/identity/app-provisioning/on-premises-migrate-microsoft-identity-manager*.

Die Verzeichnissynchronisierung über die beiden gebräuchlichen Varianten betrachten wir in Abschnitt 4.3, »Synchronisierung mit Entra Connect«, und Abschnitt 4.4, »Synchronisierung mit Entra Cloud Sync«.

4.2.2 Kennwort-Hashsynchronisierung

Mit beiden Varianten der Verzeichnissynchronisierung (Entra Connect und Entra Cloud Sync) werden auf Wunsch Änderungen an den Kennwörtern der lokalen Benutzerkonten erkannt, und das neue Kennwort wird an das zugehörige Microsoft 365-Benutzerkonto übertragen. Dabei gelten die Kennwortrichtlinien des lokalen Active Directorys, und die Richtlinien von Microsoft 365 werden außer Kraft gesetzt. Anwender müssen sich also nicht mehr unterschiedliche Kennwörter merken.

Während der Synchronisierung werden dabei nicht die Kennwörter selbst übertragen. Dies wäre auch nicht möglich, da die Domänencontroller des Active Directorys nur aus den Kennwörtern generierte Hash-Werte speichern (also eine Art Fingerabdruck). Und selbst diese Hash-Werte werden nicht übertragen, sondern sie werden nochmals dem Hash-Verfahren unterworfen. Zu Entra ID werden also gehashte Hashes der Kennwörter übertragen. Damit ist ein Zugriff auf die Klartextkennwörter nie erforderlich.

Die Synchronisierung der Kennwörter geschieht in der Standardkonfiguration nur in einer Richtung, und zwar vom lokalen Active Directory nach Microsoft 365. Ab der Aktivierung der Kennwortsynchronisierung kann der Anwender sein Kennwort in Microsoft 365 nicht mehr ändern.

Eine Ausnahme stellt die Option *Kennwortrückschreiben* dar. Dabei werden Kennwortänderungen, die der Anwender in Microsoft 365 vornimmt, an die lokale Umgebung übertragen. Das aller-

dings ist nur möglich, wenn Sie über Lizenzen vom Typ *Entra ID P1* oder *P2* verfügen, die kostenpflichtig bezogen werden müssen.

4.2.3 Passthrough-Authentifizierung (PTA)

Ist die Kennwort-Hashsynchronisierung für Sie nicht akzeptabel, können Sie davon absehen und mit der *Passthrough-Authentifizierung (PTA)* den Anwendern dennoch die Anmeldung an Microsoft 365 mit demselben Kennwort ermöglichen, das sie auch für ihr lokales Benutzerkonto verwenden. Allerdings ist die PTA nur in der Verzeichnissynchronisierungsvariante mit Entra Connect und nicht mit Entra Cloud Sync möglich. Der Ablauf ist dabei wie folgt (siehe Abbildung 4.5):

1. Der Anwender gibt bei der Anmeldung an Microsoft 365 seinen Benutzernamen und sein Kennwort ein.
2. Die Anmeldeinformationen werden an einen lokalen Agenten übertragen und von einem lokalen Domänencontroller überprüft.
3. Der Domänencontroller stellt ein Sicherheitstoken (eine Art Ausweis) aus. Dieses wird zurück an Microsoft 365 übertragen.
4. Der Anwender erhält Zugriff auf Microsoft 365.

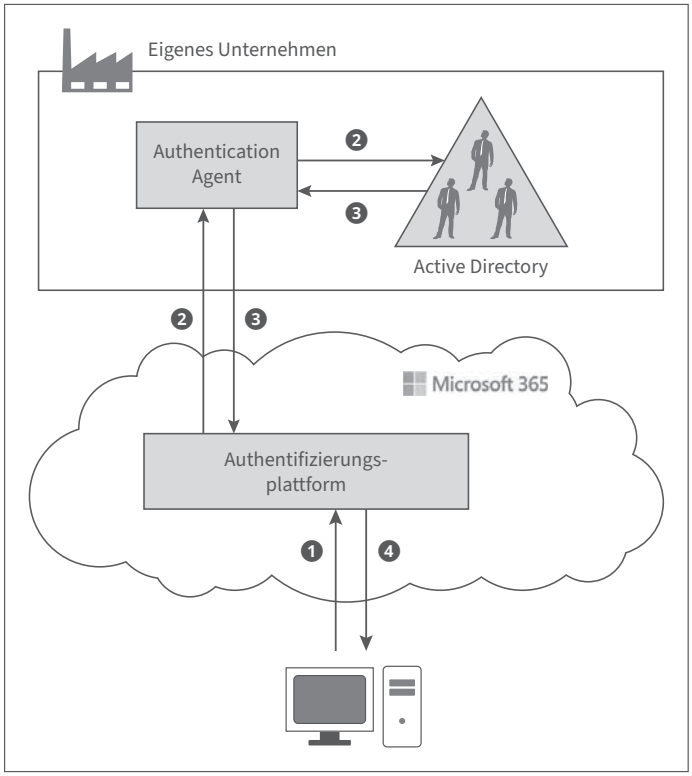

Abbildung 4.5: Passthrough-Authentifizierung

Als Agent in Schritt 2 fungiert dabei der sogenannte *Azure AD Connect Authentication Agent*, der zusammen mit Entra Connect installiert wird. Der Agent stellt eine dauerhafte Verbindung aus Ihrem lokalen Netzwerk zu Microsoft 365 her. Der Vorteil dabei: Sie benötigen keinen Reverse-Proxy in der DMZ, der es ermöglicht, vom Internet aus auf Ihre lokale Umgebung zuzugreifen.

Die Passthrough-Authentifizierung hat aber auch einen Nachteil: Fällt Ihre lokale Umgebung aus (beispielsweise weil die Internetverbindung zusammenbricht, der Azure AD Connect Authentication Agent nicht mehr reagiert oder Ähnliches), ist keine Anmeldung an Microsoft 365 mehr möglich. Entsprechend sollten Sie bei der Konfiguration für eine Hochverfügbarkeit sorgen. Dazu installieren Sie weitere Azure AD Connect Authentication Agents, die dann auch für eine Lastverteilung sorgen. Mehr dazu lesen Sie in Abschnitt 4.3.4, »Installation und Konfiguration«.

4.2.4 Single Sign-on

Grundsätzlich bedeutet Single Sign-on: Der Anwender meldet sich genau einmal an und hat dann Zugriff auf sämtliche Anwendungen und Dienste. Die Anmeldung selbst geschieht im Idealfall automatisch, sodass der Anwender weder Benutzername noch Kennwort eingeben muss. Mit Microsoft 365 ist genau dieses Verhalten allerdings nur in einer ganz bestimmten Konstellation möglich, bei der einige Voraussetzungen erfüllt sein müssen. Die möglichen Varianten samt den jeweiligen Voraussetzungen beschreibe ich in den folgenden Abschnitten.

Primäres Aktualisierungstoken

Bei einem *primären Aktualisierungstoken* (auf Englisch *Primary Refresh Token*; *PRT*) handelt es sich um die modernste Variante, die sowohl für Sie als Administrator als auch für die Anwender viele Vorteile bietet. Die Variante kommt auch ohne weitere Konfigurationsschritte zum Einsatz, sofern die Geräte der Anwender in Entra ID eingebunden sind und eines der folgenden Betriebssysteme zum Einsatz kommt:

- Windows 10 oder neuer
- Windows Server 2016 oder neuer
- iOS
- Android

Die Anmeldung erfolgt automatisch ohne die separate Eingabe von Benutzername und Kennwort. Dabei läuft im Hintergrund der Prozess aus Abbildung 4.6 ab:

1. Der initiale Schritt bei der Anforderung eines Primary Refresh Tokens unterscheidet sich, je nachdem, wie das verwendete Gerät in Entra ID eingebunden ist. Bei den Varianten *Eingebundenes Gerät (Joined Device)* und *Eingebundenes Hybridgerät (Hybrid Joined Device)* erfolgt der erste Schritt bereits während der Windows-Anmeldung des Benutzers. Bei der Variante *Registriertes Gerät (Registered Device)* erfolgt er dagegen erst dann, wenn der Anwender auf einen der Microsoft 365-Dienste zugreift (wahlweise mit einer lokal installierten Anwendung, beispielsweise der Office-Anwendungen, oder im Browser).

❷ Bei Entra ID wird das Primary Refresh Token angefordert.

❸ Das Primary Refresh Token wird lokal in einem Cache vorgehalten, für den zukünftigen Fall, dass einmal kein Internetzugang vorhanden ist. Außerdem erfolgt automatisch die regelmäßige Aktualisierung des Tokens.

Zur Einbindung der Geräte in Entra ID sind gewisse Voraussetzungen zu erfüllen. Diese beschreibe ich ausführlich in Abschnitt 16.1, »Geräte in Entra ID«.

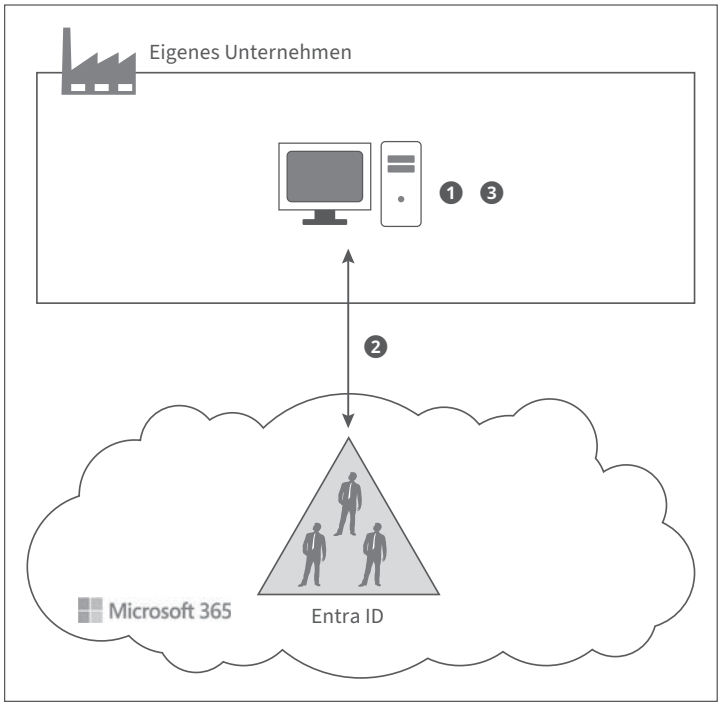

Abbildung 4.6: Primary Refresh Token

Seamless Single Sign-on

Sind die Voraussetzungen für Single-Sign-on auf Basis des PRT nicht gegeben, beispielsweise weil ein zu altes Betriebssystem verwendet oder das Gerät nicht in Entra ID aufgenommen werden kann, könnte die Alternative *Seamless Single Sign-on* sein.

Bei diesem Verfahren wird vermieden, dass der Anwender sein Kennwort eingeben muss. Abhängig davon, über welche URL der Anwender auf die Microsoft 365-Dienste zugreift, entfällt auch die Angabe des Benutzernamens. Voraussetzung dafür ist, dass in der URL der gewünschte Microsoft 365-Mandant referenziert wird, wie beispielsweise bei diesen URLs:

- *https://outlook.office365.com/beispielag.de*
- *https://beispielag.sharepoint.com*
- *https://portal.azure.com/beispielag.de*

Verwendet der Anwender dagegen eine allgemeine URL, wie beispielsweise *https://outlook.office365.com*, muss er zumindest seinen Benutzernamen angeben.

Damit Seamless Single Sign-on auch tatsächlich funktioniert, müssen Sie gegebenenfalls unter Windows einige Anpassungen vornehmen:

- **Alle Browser**

  Suchen Sie in den Windows-Einstellungen nach den **Internetoptionen**, und konfigurieren Sie diese Punkte:

  – Fügen Sie auf der Registerkarte **Sicherheit** innerhalb der Zonenkonfiguration zur Zone **Lokales Intranet** die folgende URL hinzu: `https://autologon.microsoftazuread-sso.com` (siehe Abbildung 4.7).

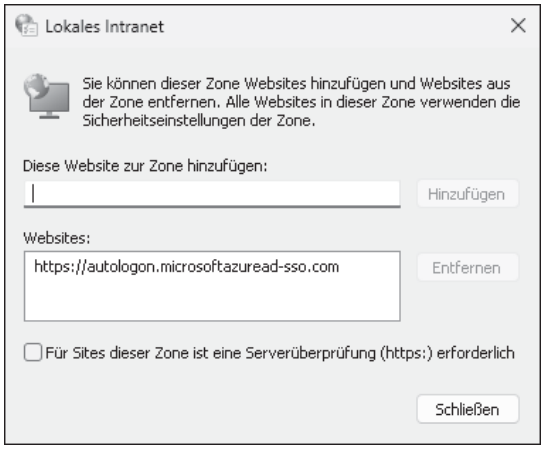

Abbildung 4.7: Zonenkonfiguration

  – Aktivieren Sie in derselben Zone die Option **Statusleistenupdates über Skript zulassen**.

- **Firefox**

  Öffnen Sie die Seite *about:config*. Suchen Sie dann nach **network.negotiate-auth.trusted-uris**, und fügen Sie dort die URL *https://autologon.microsoftazuread-sso.com* als Wert hinzu (siehe Abbildung 4.8).

Abbildung 4.8: Firefox-Konfiguration

Seamless Single Sign-on ist nur auf Clients möglich, die Domänenmitglied sind und außerdem über eine direkte Verbindung zu einem Domänencontroller verfügen. So geht es also beispielsweise nicht aus dem Heimnetzwerk ohne VPN-Verbindung. Anwender mit Clients, die diese Anforderung nicht erfüllen, werden aufgefordert, ihr Kennwort einzugeben.

Der Prozess beim Anmelden ist dabei wie folgt (siehe Abbildung 4.9):

❶ Der Client fordert automatisch ein Kerberos-Sicherheitstoken von einem Domänencontroller an.

❷ Das Sicherheitstoken wird an Microsoft 365 übertragen.

❸ Das Token wird überprüft, und die Anmeldung wird vorgenommen.

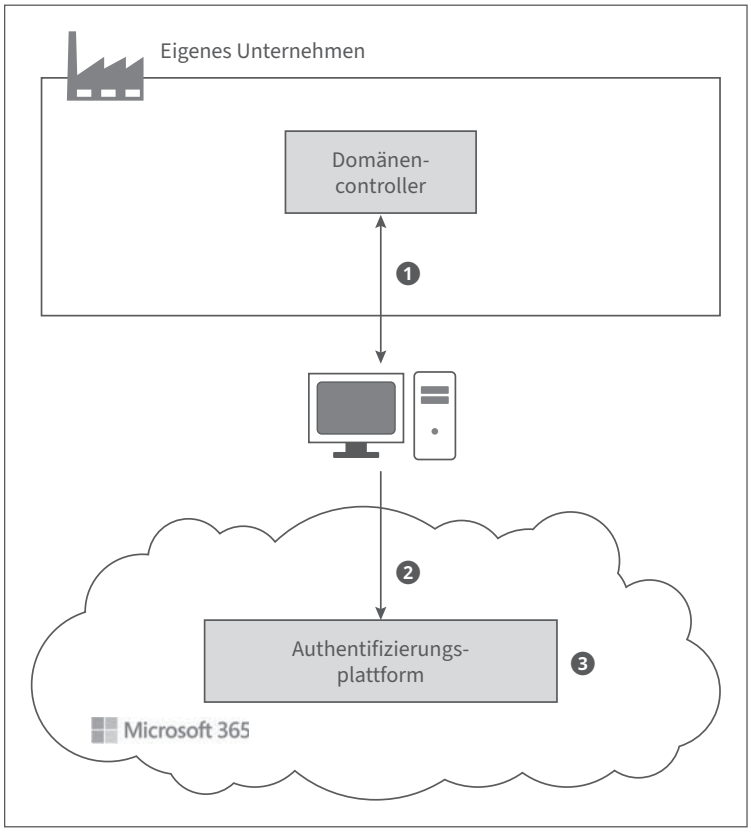

Abbildung 4.9: Seamless Single Sign-on

Single Sign-on im Identitätsverbund

Von Beginn an bietet Microsoft 365 ein *Single Sign-on im Identitätsverbund*. Dieser Verbund wird auf Basis von *AD FS (Active Directory Federation Services)* aufgebaut. Im Vergleich zu Seamless Single Sign-on ist der Aufwand, den Sie in Ihrer lokalen Infrastruktur treiben müssen, deutlich höher, denn es ist neben der Verzeichnissynchronisierung eine (meist hochverfügbare) AD FS-Umgebung erforderlich. Gerade für kleinere Firmen ist dies ein wichtiges Merkmal. Single Sign-on er-

fordert dagegen AD FS, das typischerweise auf mehreren Servern eingerichtet wird. Diese Server können zwar gerne virtuell sein, jedoch müssen sie dennoch lizenziert sein sowie überwacht und gewartet werden.

Sollte die komplexe AD FS-Infrastruktur ausfallen oder kann sie aufgrund von Problemen mit Ihrem Internetprovider nicht erreicht werden, können sich Ihre Anwender nicht mehr an Microsoft 365 anmelden.

Grundsätzlich gilt die Empfehlung, Single Sign-on im Identitätsverbund nur dann einzusetzen, wenn es einen wirklich triftigen Grund dafür gibt, denn der Kosten- und Verwaltungsaufwand für die dabei notwendige AD FS-Umgebung ist recht hoch.

Aufgrund der Komplexität dieses Themas beschreibe ich die Einrichtung eines Identitätsverbunds in einem separaten Abschnitt (siehe Abschnitt 4.5).

4.2.5 Integrationsszenarien im Vergleich

Mit verschiedenen Kombinationen aus den in den vorangegangenen Abschnitten eingeführten Komponenten können Sie nun die für Ihr Unternehmen am besten geeignete Lösung für die Entra ID-Integration bestimmen. Zur Auswahl stehen dabei die folgenden Szenarien:

- **Nur Microsoft-Online-IDs (keine Verzeichnissynchronisierung)**
  In diesem Szenario legen Sie im Microsoft 365-Verzeichnisdienst manuell Benutzerkonten für Ihre Anwender an. Dies können Sie beispielsweise ganz klassisch über das Microsoft 365 Admin Center durchführen, wie ich es in Abschnitt 2.5.2, »Benutzer anlegen«, beschrieben habe. Eine Alternative zur Automatisierung wäre die PowerShell, wie in Abschnitt 3.13.2, »Benutzer anlegen«, dargestellt.

  Ihre Anwender melden sich an Microsoft 365 über das Benutzerkonto aus dem Microsoft 365-Verzeichnisdienst an. Die Authentifizierung erfolgt dabei also nicht im lokalen Active Directory, sondern direkt in Microsoft 365.

  Wenn Sie sich dieses Szenario durch den Kopf gehen lassen, erkennen Sie verschiedene Nachteile, beispielsweise:

  - Die Anwender müssen mit zwei Identitäten umgehen – einmal mit der lokalen Identität und einmal mit der Identität aus Microsoft 365. Sie müssen also auch mit zwei unterschiedlichen Kennwörtern und manchmal auch mit unterschiedlichen Benutzernamen umgehen können und erkennen, wann sie welches einzugeben haben.
  - Identische Kennwörter sind dabei oft nicht möglich, da unterschiedliche Kennwortrichtlinien und Ablaufzeiten bestehen. Vergisst ein Anwender sein Kennwort, muss es potenziell an zwei unterschiedlichen Stellen zurückgesetzt werden.

  Dieses Szenario hat aber auch zwei große Vorteile:

  - Zu Beginn fällt der geringste Konfigurationsaufwand an.
  - Es kann direkt nach dem Anlegen eines Microsoft 365-Mandanten angewandt werden, ohne dass an der lokalen Umgebung Änderungen vorgenommen werden müssen.

  - Möglicherweise verzichtet Ihr Unternehmen ganz auf ein Active Directory, weil beispielsweise alle Mitarbeiter unterwegs sind und eine lokale IT-Infrastruktur nicht erforderlich ist.

- **Verzeichnissynchronisierung** (AD-Sync)
  Es gibt sie wahlweise in den Varianten Entra Connect und Entra Cloud Sync (siehe auch Abschnitt 4.2.1, »Verzeichnissynchronisierung«, für die Unterschiede und Einschränkungen).
- **Verzeichnissynchronisierung + Kennwort-Hashsynchronisierung** (AD-Sync + KW-Sync)
- **Verzeichnissynchronisierung + Passthrough-Authentifizierung** (AD-Sync + Passthrough)
- **Verzeichnissynchronisierung + Identitätsverbund** (AD-Sync + Identitätsverbund)
  Über ein Vertrauensverhältnis zwischen Microsoft 365 und Ihrer lokalen Umgebung erkennt Microsoft 365 die lokale Anmeldung mithilfe eines speziellen Sicherheitstokens an. Für die Microsoft 365-Dienste sind jedoch Benutzerkonten in Entra ID erforderlich, weshalb dort auch die Benutzerkonten über die Active Directory-Synchronisierung angelegt werden müssen. Dieses Szenario erfordert eine relativ aufwendige Konfiguration auf Basis der *Active Directory Federation Services* (*AD FS* oder auf Deutsch *Active Directory-Verbunddienste*). Wie das geht, werde ich Ihnen in Abschnitt 4.5, »Identitätsverbund«, zeigen.

Einen Vergleich der Szenarien finden Sie in Tabelle 4.3.

Kriterium	Nur MS-Online-Identität (kein AD-Sync)	AD-Sync	AD-Sync + KW-Sync	AD-Sync + Passthrough	AD-Sync + Identitätsverbund
Zielgruppe	kleine Unternehmen	mittlere und große Unternehmen mit eigenem Active Directory	mittlere und große Unternehmen mit eigenem Active Directory	mittlere und große Unternehmen mit eigenem Active Directory	große Unternehmen mit eigenem Active Directory
Varianten für Single Sign-on	– Primary Refresh Token	– Primary Refresh Token	– Primary Refresh Token – Seamless Single Sign-on	– Primary Refresh Token – Seamless Single Sign-on	– Primary Refresh Token – Seamless Single Sign-on – Identitätsverbund
Kennwortspeicherung	separate Kennwörter lokal + Microsoft 365	separate Kennwörter lokal + Microsoft 365	lokales Kennwort + Kennwort-Hash in Microsoft 365	nur lokales Kennwort	nur lokales Kennwort

Tabelle 4.3: Vergleich der Integrationsszenarien

Kriterium	Nur MS-Online-Identität (kein AD-Sync)	AD-Sync	AD-Sync + KW-Sync	AD-Sync + Passthrough	AD-Sync + Identitätsverbund
Anmeldung mit lokalem Kennwort möglich?	nein	nein	ja	ja	ja
Ort der Authentifizierung	lokal + Microsoft 365	lokal + Microsoft 365	lokal + Microsoft 365	nur lokal	nur lokal
Welche Kennwortrichtlinien gelten?	lokal + Microsoft 365	lokal + Microsoft 365	nur lokal	nur lokal	nur lokal
Ort der Benutzerverwaltung	lokal + Microsoft 365	nur lokal	nur lokal	nur lokal	nur lokal
Zusätzliche lokale Installation erforderlich?	nein	ja, Entra Connect oder Agent von Entra Cloud Sync	ja, Entra Connect oder Agent von Entra Cloud Sync	ja, Entra Connect	ja, Entra Connect oder Agent von Entra Cloud Sync + AD FS
minimale lokale Serveranzahl	0	Entra Connect oder Agent von Entra Cloud Sync auf einem bestehenden Server im internen Netz	Entra Connect oder Agent von Entra Cloud Sync auf einem bestehenden Server im internen Netz	Entra Connect auf einem bestehenden Server im internen Netz	– Entra Connect oder Agent von Entra Cloud Sync auf einem bestehenden Server im internen Netz – AD FS auf einem bestehenden Server im internen Netz – Proxy auf einem bestehenden Server in der DMZ
Öffentliches SSL-Zertifikat erforderlich?	nein	nein	nein	nein	ja

Tabelle 4.3: Vergleich der Integrationsszenarien (Forts.)

Kriterium	Nur MS-Online-Identität (kein AD-Sync)	AD-Sync	AD-Sync + KW-Sync	AD-Sync + Passthrough	AD-Sync + Identitätsverbund
typische lokale Serveranzahl	0	ein Server für Entra Connect oder Agent von Entra Cloud Sync im internen Netz	ein Server für Entra Connect oder Agent von Entra Cloud Sync im internen Netz	– ein Server für Entra Connect im internen Netz – ein Server für Hochverfügbarkeit mit PTA im internen Netz	– ein Server für Entra Connect oder Agent von Entra Cloud Sync im internen Netz – zwei Server für AD FS im internen Netz – zwei Server für Proxys in der DMZ
Anmeldung an Microsoft 365 noch möglich, wenn lokale Umgebung komplett ausfällt?	ja	ja	ja	nein	nein

Tabelle 4.3: Vergleich der Integrationsszenarien (Forts.)

Empfehlung

Grundsätzlich empfehle ich Ihnen, die Variante Verzeichnissynchronisierung mit der Kennwort-Hashsynchronisierung besonders in Betracht zu ziehen (sofern Sie über ein Active Directory verfügen), denn durch sie erhalten Sie eine ganze Reihe an Vorteilen, insbesondere diese:

- Die erforderlichen Komponenten in der lokalen IT-Infrastruktur sind gering – außer dem Entra Connect oder dem Agenten von Entra Cloud Sync sind keine weiteren Komponenten erforderlich.
- Die Authentifizierung in Microsoft 365 ist selbst dann möglich, wenn die komplette lokale Infrastruktur ausfällt.
- Für die Authentifizierung sind keine Zugriffe von den Clouddiensten auf Ihre lokale Infrastruktur erforderlich.
- Da Hash-Werte der Kennwörter in Microsoft 365 verfügbar sind, können die Werte mit im Internet veröffentlichten Passwort-Listen verglichen werden (indem von den Kennwörtern dort auf dieselbe Art Hash-Werte generiert werden), um Sie gegebenenfalls darauf hinzuweisen, dass die Benutzerdaten kompromittiert wurden. Mehr dazu lesen Sie in Abschnitt 14.2.2, »Bedingter Zugriff«.

4.3 Synchronisierung mit Entra Connect

Wie ich in Abschnitt 4.2.1, »Verzeichnissynchronisierung«, beschrieben habe, ist die Verzeichnissynchronisierung mit Entra Connect im Vergleich zur Variante Entra Cloud Sync (siehe Abschnitt 4.4, »Synchronisierung mit Entra Cloud Sync«) funktional leistungsfähiger, dafür aber auch in der Einrichtung etwas komplexer. Entra Connect wird mit je einem Connector zum lokalen Active Directory und zum Microsoft 365 Entra ID eingerichtet (siehe Abbildung 4.10).

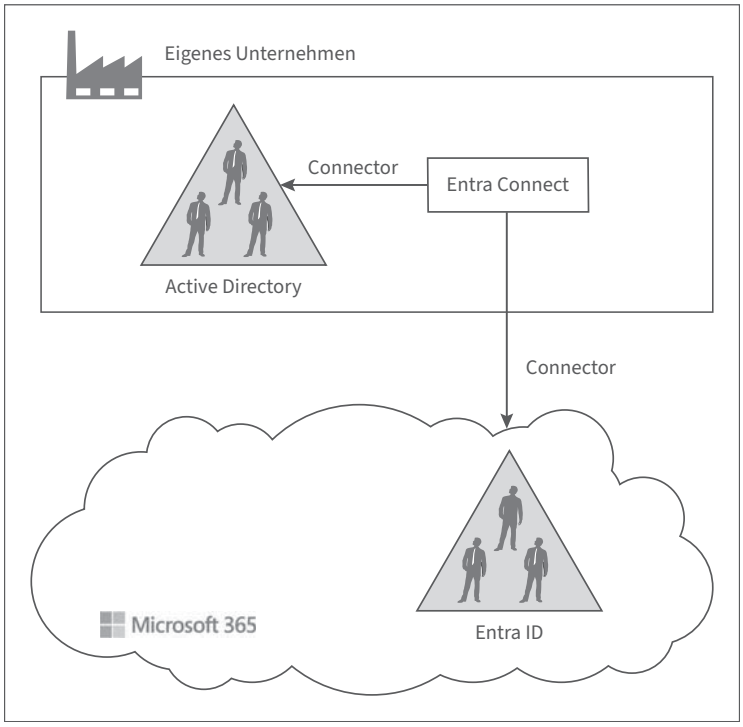

Abbildung 4.10: Entra Connect mit Connectors

Über die Connectors greift der Synchronisierungsdienst auf die beiden Verzeichnisse zu. Dazu ist in beiden Verzeichnissen jeweils ein Benutzerkonto mit den erforderlichen Berechtigungen erforderlich, die Entra Connect verwendet, um Daten auszulesen (beispielsweise die Benutzerkonten aus dem Active Directory) und gegebenenfalls zu ändern oder zu löschen (beispielsweise die Telefonnummer eines lokalen Benutzerkontos in Entra ID).

Entra Connect läuft im Hintergrund und gleicht in der Standardkonfiguration in einem regelmäßigen Intervall von 30 Minuten automatisch Elemente Ihres Active Directorys mit dem Verzeichnisdienst von Microsoft 365 ab. Betroffen sind dabei die folgenden Objekte:

- Benutzerkonten
- Gruppen
- Kontakte
- Computer
- Geräte

Eine Auflistung der synchronisierten Attribute finden Sie unter der folgenden URL:

https://learn.microsoft.com/de-de/entra/identity/hybrid/connect/reference-connect-sync-attributes-synchronized

Wollen Sie nicht alle hier aufgeführten Attributwerte synchronisieren, beispielsweise weil Sie nicht möchten, dass die Telefonnummern in die Cloud wandern, ist eine Auswahl der zu synchronisierenden Attribute bis zu einem gewissen Grad über den Konfigurationsassistenten von Entra Connect möglich. Doch sollten Sie sich die Deaktivierung von einzelnen Attributen in der Praxis gut überlegen: Die Gefahr ist groß, ein Attribut abzuwählen, das heute oder in Zukunft von den Microsoft 365-Diensten benötigt wird, um eine korrekte Funktionsweise zu gewährleisten. Überlegen Sie deshalb nicht, welche Attribute Sie mindestens synchronisieren müssen, sondern welche Attribute Sie unter keinen Umständen synchronisieren wollen. Diese Vorgehensweise minimiert Probleme enorm. Natürlich dürfen Sie sich dann allerdings auch nicht wundern, wenn beispielsweise die Telefonnummern in der globalen Adressliste von Exchange Online nicht angezeigt werden, falls Sie sie von der Synchronisierung ausgenommen haben.

Neu angelegte Objekte im lokalen Active Directory werden automatisch beim nächsten Synchronisierungslauf im Microsoft 365-Verzeichnisdienst angelegt, beispielsweise die Benutzerkonten neuer Mitarbeiter. Löschen oder ändern Sie lokal ein Objekt, wird es auch in Microsoft 365 gelöscht oder geändert. Welche Objekte und welche Attribute von links nach rechts oder von rechts nach links synchronisiert werden, hängt von einem Regelwerk und verschiedenen Filtern ab. Grundsätzlich werden dabei drei unterschiedliche Verfahren zur Filterkonfiguration unterstützt:

- Organisationseinheiten filtern
- Domänen filtern
- attributbasierte Filterung

Die Synchronisierung selbst wird grundsätzlich als *Pushsynchronisierung* ausgeführt – ausgehend von Ihrem Active Directory hin zu Microsoft 365. Es gibt jedoch Ausnahmen, bei denen manche Active Directory-Eigenschaften von Entra ID zurück in Ihr Active Directory synchronisiert werden, beispielsweise diese:

- **vollständige Exchange-Hybridkonfiguration** (siehe Abschnitt 6.10)
- **Kennwort zurückschreiben:** Dabei werden Kennwortänderungen, die der Anwender in Microsoft 365 vornimmt, an die lokale Umgebung übertragen. (Das ist nur möglich, wenn Sie über Lizenzen vom Typ Entra ID P1 oder P2 verfügen, die separat eingekauft werden müssen – beziehungsweise sind diese Bestandteile der größeren Basislizenzen.)
- **Geräte zurückschreiben:** Auch dies ist eine Funktionalität von Entra ID P1 und P2, die es ermöglicht, im Entra ID registrierte Objekte lokal für einen bedingten Zugriff zu konfigurieren.

Nach der Aktivierung der Active Directory-Synchronisierung verwalten Sie die synchronisierten Objekte primär nach wie vor mit den Verwaltungstools des lokalen Active Directorys. Die Benutzerverwaltung von Microsoft 365 verwenden Sie dagegen in erster Linie für die Lizenzierung der synchronisierten Benutzerkonten.

Die Synchronisierung ist insbesondere in folgenden Szenarien eine Voraussetzung:

- für die Passthrough-Authentifizierung (siehe Abschnitt 4.2.3)
- für Seamless Single Sign-on (siehe Abschnitt 4.2.4)
- für die Einrichtung eines Identitätsverbunds (siehe Abschnitt 4.5)
- für die Einrichtung einer vollständigen Exchange-Hybridkonfiguration (siehe Abschnitt 6.10, »Vollständige Exchange-Hybridkonfiguration«)
- für die mehrstufige Exchange-Migration (siehe Abschnitt 6.9, »Exchange-Migration«)

4.3.1 Der Synchronisierungsvorgang

Nachdem Sie das Verzeichnissynchronisierungstool installiert und konfiguriert haben, erfolgt eine vollständige Synchronisierung der unterstützten Objekte. Diese initiale Synchronisierung (*Full Sync*) dauert am längsten. Bei den weiteren Synchronisierungsläufen werden nur die Änderungen berücksichtigt (*Delta Sync*).

Während der Synchronisierung werden in der Standardkonfiguration zwei Strategien angewandt, um die Objekte aus dem lokalen Active Directory mit dem Verzeichnisdienst von Microsoft 365 abzugleichen:

1. **GUID-Vergleich**
   Wird ein Objekt durch das Synchronisierungstool im Microsoft 365-Verzeichnisdienst angelegt, erhält es dort eine Markierung mit einem eindeutigen Merkmal des entsprechenden Objekts aus dem lokalen Active Directory (*Net-ID* genannt). Daran wird es bei zukünftigen Synchronisierungsverläufen erkannt. In der Standardkonfiguration wird hierbei bei Benutzerkonten der Wert des Attributs `ms-DS-ConsistencyGUID` herangezogen – bei allen anderen Objekttypen wird das Attribut `ObjectId` verwendet. Wurde das Attribut `ms-DS-ConsistencyGUID` bisher im Active Directory noch nicht verwendet, wird es nun automatisch mit Werten gefüllt. Die jeweiligen Werte der lokalen Benutzerkonten werden im zugehörigen Entra ID-Benutzerkonto im Attribut `ImmutableId` hinterlegt (in einer Base64-Codierung).
2. **SMTP-Vergleich**
   Wird im Microsoft 365-Verzeichnisdienst kein Objekt mit passender GUID gefunden, werden (sofern vorhanden) die primären SMTP-Adressen verglichen.

   Dieser Fall tritt beispielsweise dann auf, wenn Sie schon vor der Aktivierung der Synchronisierung im Microsoft 365-Mandanten Benutzerkonten mit entsprechenden SMTP-Adressen anlegen. Zuständig ist das Active Directory-Attribut `proxyAddresses`. Die primäre SMTP-Adresse ist dort als Wert in der Form `SMTP:benutzer@domäne` hinterlegt. SMTP muss dabei für die primäre Adresse großgeschrieben sein.

   Während der Synchronisierung werden passende Microsoft 365-Benutzer dann mit den lokalen Active Directory-Benutzern verbunden.
3. **Benutzerprinzipalnamen-Vergleich**
   Der SMTP-Vergleich kann nicht immer vorgenommen werden, beispielsweise weil Ihren Benutzerkonten im Entra ID keine Lizenz für Exchange Online zugewiesen wurde und Sie damit auch

keine SMTP-Adresse vergeben können. Schlägt der SMTP-Vergleich fehl, wird der *Benutzerprinzipalname (User Principal Name; UPN)* für eine Zuordnung herangezogen.

Das Intervall zwischen den Synchronisierungsverläufen beträgt in der Standardkonfiguration 30 Minuten. Allerdings können Sie die Synchronisierung bei Bedarf manuell starten, beispielsweise wenn das Benutzerkonto des neuen Mitarbeiters sofort in Microsoft 365 verfügbar sein soll und nicht erst nach bis zu 30 Minuten (siehe Abschnitt 4.3.6, »Manueller Start der Synchronisierung«).

4.3.2 Planung und Vorbereitung

Die Einrichtung der Synchronisierung ist ein wichtiger Schritt bei der Anbindung Ihres Microsoft 365-Mandanten an das lokale Active Directory. Dabei müssen Sie aber einige Punkte berücksichtigen, die ich Ihnen in diesem Abschnitt erläutern werde.

Einschränkungen

- **Anzahl der Active Directory-Objekte**
  Beim Entra Connect gibt es zwei Grenzwerte bei der Anzahl von Active Directory-Objekten. Keine Probleme treten auf bei bis zu 300.000 Objekten (Benutzer, Gruppen, Kontakte, Geräte), vorausgesetzt, Sie haben in Ihrem Microsoft 365-Mandanten eine eigene Domäne verifiziert – ansonsten gilt eine Grenze von 50.000 Objekten.

  Werden mehr als 300.000 Objekte synchronisiert, kontaktieren Sie den Microsoft 365-Kundendienst für eine entsprechende Freischaltung Ihres Microsoft 365-Mandanten (siehe Abschnitt 2.9, »Problembehebung«). Bei mehr als 500.000 Objekten benötigen Sie *Microsoft 365*-, *EMS*- oder *Entra ID*-Lizenzen.

  Werden weniger als 100.000 Objekte synchronisiert, kann das Verzeichnissynchronisierungstool den automatisch mitinstallierten *Microsoft SQL Server Express LocalDB* verwenden. Bei mehr Objekten ist eine Instanz der »großen« SQL Server erforderlich, die gesondert bereitgestellt und lizenziert werden muss.
- **Administration von Benutzerkonten**
  Es ist zwar nicht wirklich eine Einschränkung, aber Sie sollten es dennoch beachten: Sobald die Synchronisierung aktiviert ist, können Sie viele Eigenschaften der Benutzerkonten nur noch über die lokalen Active Directory-Tools und nicht mehr im Microsoft 365 Admin Center bearbeiten (siehe Abbildung 4.11).

  Es dürfte zunächst eher eine Erleichterung sein, mit den gewohnten Werkzeugen einfach weiterarbeiten zu können. Etwas problematischer wird die Sache, wenn Sie Exchange Online einsetzen. In diesem Fall können von Microsoft 365-Seite aus viele Exchange-Attribute der Benutzerkonten nicht geändert werden, beispielsweise die E-Mail-Adressen. Solche Attribute müssen dann ebenfalls mit lokal vorhandenen Tools verwaltet werden, was sich schwierig gestalten kann, wenn Sie lokal keinen Exchange Server (mehr) haben. Lesen Sie hierzu auch Abschnitt 6.2.3, »Ändern von Exchange-Attributen mit aktivierter Verzeichnissynchronisierung«.

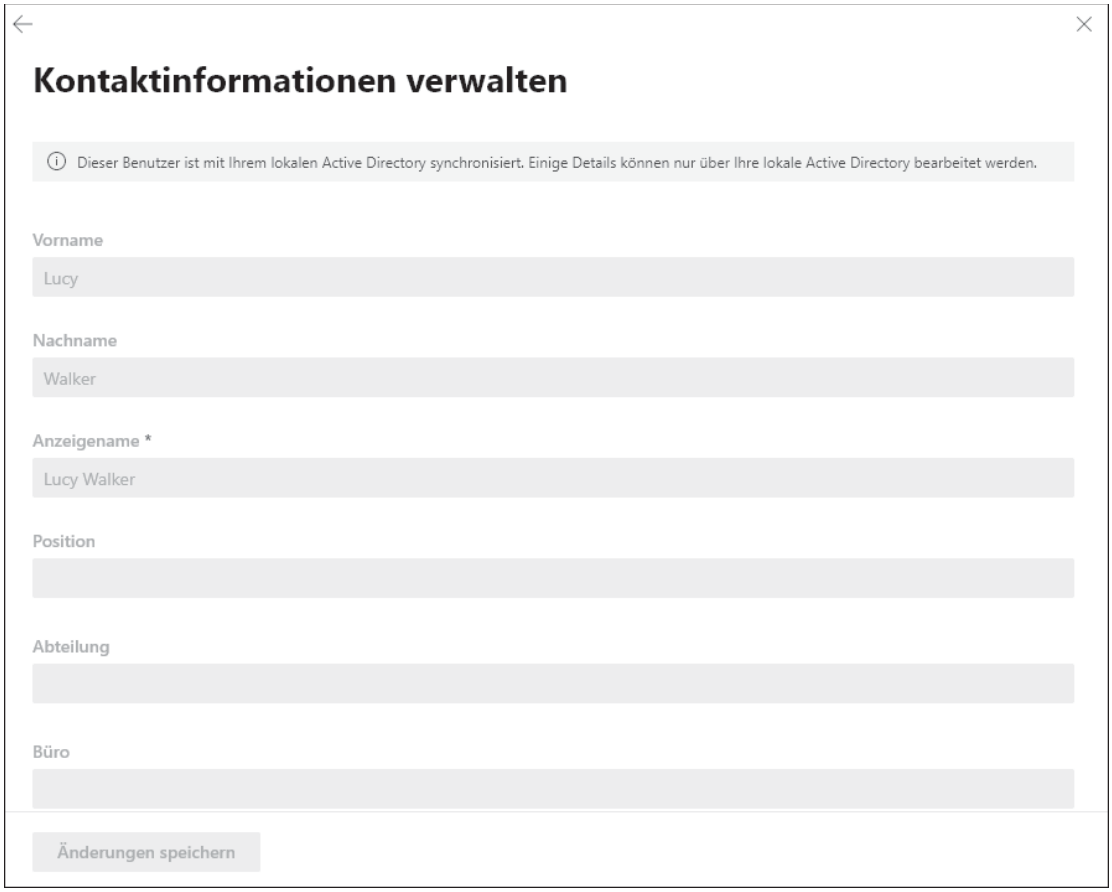

Abbildung 4.11: Eingeschränkte Bearbeitung von Benutzerkonten im Microsoft 365 Admin Center

Neue Benutzerkonten legen Sie nach der Aktivierung der Synchronisierung auch nur noch lokal im Active Directory an und nicht mehr im Microsoft 365 Admin Center. Benutzerkonten, die Sie dennoch direkt in Microsoft 365 erstellen, werden nicht auch automatisch in Ihrem Active Directory angelegt.

Dennoch kann es sinnvoll sein, einzelne Benutzer direkt im Microsoft 365 Admin Center anzulegen, beispielsweise für administrative Benutzer und für externe Anwender, die nur Zugriff auf Microsoft 365, aber nicht auf das lokale Netzwerk bekommen sollen.

- **Exchange Online-Lizenzierung**
  Angenommen, Sie verfügen über einen lokalen Exchange Server und verwenden die Verzeichnissynchronisierung. Weisen Sie dann einem synchronisierten Benutzer eine Lizenz zu, die Exchange Online umfasst, wird für ihn nicht mehr automatisch ein Postfach angelegt, sofern er bereits über ein lokales Postfach verfügt. In der Verwaltungsoberfläche von Exchange Online erscheint dann für den Anwender kein Postfach (siehe Abbildung 4.12).

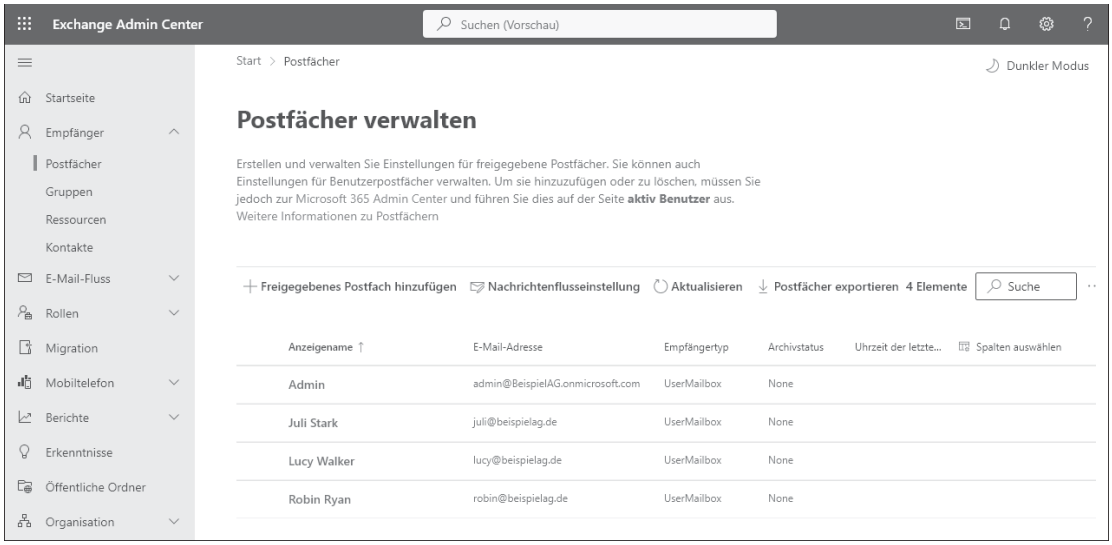

Abbildung 4.12: Die Verwaltungsoberfläche von Exchange Online

Das hat auch seinen Grund: Wollten Sie später das lokale Postfach zu Exchange Online verschieben, ginge das nicht mehr, da dort für den Benutzer bereits ein Postfach vorhanden wäre.

Vorbereitungen

Bevor Sie die Active Directory-Synchronisierung einrichten, sollten Sie einige Dinge überprüfen:

- **Active Directory-Attribute lokaler Benutzerkonten**
  Vor der Aktivierung der Synchronisierung sollten Sie sicherstellen, dass die Benutzerprinzipalnamen (UPN) der lokalen Benutzerkonten geeignet gesetzt sind. Die Benutzerprinzipalnamen der lokalen Benutzerkonten fungieren in Microsoft 365 als Benutzernamen. Dazu müssen sie folgende Voraussetzungen erfüllen:
  - Der Benutzerprinzipalname muss vergeben sein.
  - Die Domänen der Benutzerprinzipalnamen sind in Ihrem Microsoft 365-Mandanten verifiziert (siehe Abschnitt 2.4.2). Das schließt Domänen aus, die im Internet nicht routbar sind, beispielsweise solche mit der Endung *.local* und *.intra*.
  - Im Idealfall ist der Benutzerprinzipalname identisch mit der E-Mail-Adresse des Anwenders. Dies hat nicht nur den praktischen Grund, dass sich der Anwender nicht einen speziellen Anmeldenamen merken muss. Die Anmeldefenster im Kontext von Microsoft 365 haben an verschiedenen Stellen ein Feld, bei dem der Anwender aufgefordert wird, seine E-Mail-Adresse einzugeben. Ein Beispiel sehen Sie in Abbildung 4.13 bei der Anmeldung an Microsoft 365 von Word aus. Rein technisch betrachtet, ist das nicht korrekt, denn der Anwender muss nicht seine E-Mail-Adresse, sondern seinen Benutzerprinzipalnamen angeben. Um solchen Verwirrungen vorzubeugen, empfiehlt es sich deshalb, gleich auf die E-Mail-Adresse zu setzen.

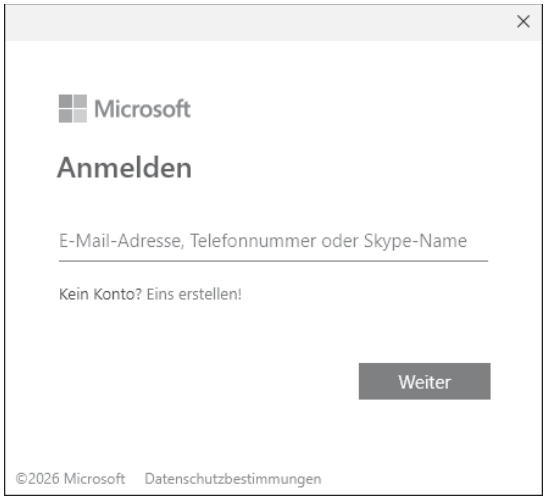

Abbildung 4.13: Anmeldefenster in Word

– Sollte es unbedingt erforderlich sein, können Sie als Benutzernamen der Microsoft 365-Benutzerkonten statt des Benutzerprinzipalnamens der lokalen Active Directory-Benutzer auch ein anderes Attribut einsetzen (beispielsweise `mail`). Das sollte aber eher ein Ausnahmefall bleiben. Eine Liste der Probleme, die Sie sich dadurch einhandeln, – und wie Sie diese gegebenenfalls in den Griff bekommen – finden Sie hier:

  https://learn.microsoft.com/de-de/windows-server/identity/ad-fs/operations/configuring-alternate-login-id

Benötigen Sie ein alternatives Benutzerprinzipalnamen-Suffix (beispielsweise weil Ihre Domäne *beispielag.local* heißt und Sie jetzt bei den Benutzerprinzipalnamen *beispielag.de* verwenden wollen), gehen Sie wie folgt vor:

– Öffnen Sie die Managementkonsole **Active Directory-Domänen und -Vertrauensstellungen** (siehe Abbildung 4.14). Diese finden Sie im Zweifelsfall auf einem Domänencontroller.

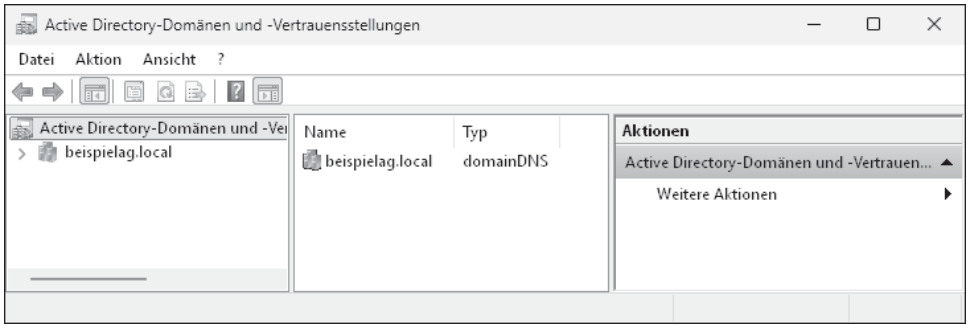

Abbildung 4.14: Active Directory-Domänen und -Vertrauensstellungen

– Klicken Sie mit der rechten Maustaste in der linken Navigation auf **Active Directory-Domänen und -Vertrauensstellungen**, und wählen Sie im Kontextmenü die **Eigenschaften** (siehe Abbildung 4.15).

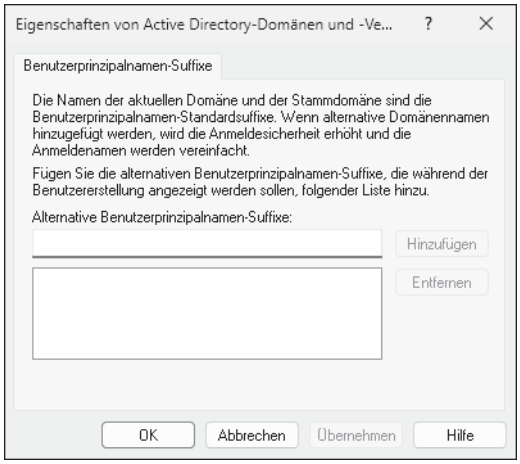

Abbildung 4.15: Hinzufügen eines neuen Benutzerprinzipalnamen-Suffixes

– Fügen Sie im erscheinenden Fenster ein alternatives Benutzerprinzipalnamen-Suffix hinzu. Dieses können Sie dann bei den Benutzerkonten auswählen.

Wie Sie die Benutzerprinzipalnamen mithilfe der PowerShell automatisiert vergeben, lesen Sie in Abschnitt 3.14.2, »Anwendung«.

Was sind Benutzerprinzipalnamen (UPNs)?

Benutzerkonten im Active Directory haben potenziell zwei Benutzernamen, wie Sie in Abbildung 4.16 sehen:

- **Benutzeranmeldename** (= Benutzerprinzipalname, User Principal Name/UPN)
  Dieser Benutzerprinzipalname ist optional und hat die Form einer E-Mail-Adresse: *Benutzer@Domäne*, also beispielsweise *lucy@beispielag.de*. Oftmals ist die E-Mail-Adresse des Benutzers auch identisch mit diesem Benutzerprinzipalnamen – das muss aber nicht so sein. Der Teil hinter dem Klammeraffen wird auch allgemein als *Benutzerprinzipalnamen-Suffix* bezeichnet, da er nicht identisch mit dem eigentlichen Domänennamen sein muss.
- **Benutzeranmeldename (Prä-Windows 2000)** (= *SAM Account Name*)
  Jedes Benutzerkonto im Active Directory verfügt über einen SAM Account Name. Er hat die Form *Domäne\Benutzer*, also beispielsweise *BeispielAG\Lucy*.

Für Microsoft 365 spielt der zweite Anmeldename, also der SAM Account Name, keine Rolle. Legen Sie in Microsoft 365 ein Benutzerkonto an, vergeben Sie auch nur den Benutzerprinzipalnamen als Benutzernamen.

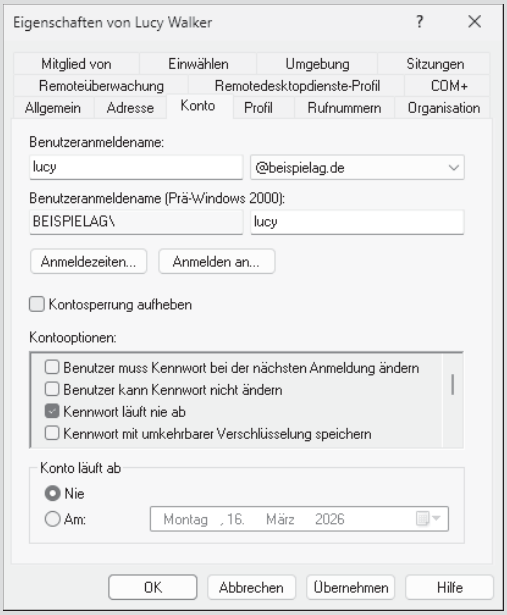

Abbildung 4.16: Benutzerkontoeigenschaften im Active Directory

4.3.3 Überprüfen der lokalen Umgebung

Damit Sie die Active Directory-Synchronisierung einrichten können, muss Ihre lokale Umgebung einige Voraussetzungen erfüllen. Microsoft stellt für die Überprüfung der lokalen Umgebung ein Tool bereit, mit dem Sie ohne großen Aufwand Ihre lokale Umgebung schon vor Konfigurationsänderungen auf mögliche Problemstellen hin untersuchen können. So erhalten Sie rechtzeitig Hinweise, was Sie zunächst noch ändern sollten, bevor Sie mit der eigentlichen Konfiguration beginnen.

IdFix DirSync Error Remediation Tool

Speziell für das Überprüfen des Active Directorys und der darin enthaltenen Objekte bietet sich das *IdFix DirSync Error Remediation Tool* an. Es zeigt Ihnen Objekte, die bei der Synchronisierung Probleme verursachen würden, und schlägt auch entsprechende Abhilfe vor (siehe Abbildung 4.17).

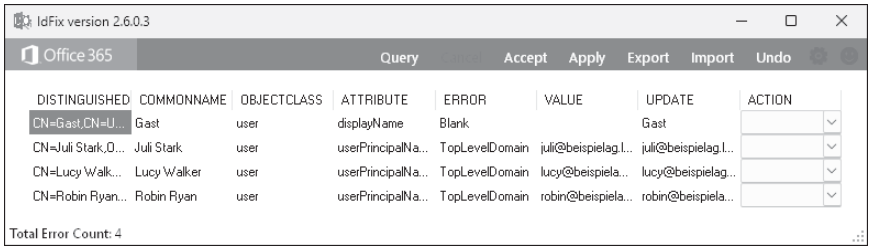

Abbildung 4.17: IdFix hat Probleme erkannt.