


Diese Leseprobe haben Sie beim
 edv-buchversand.de heruntergeladen.
 Das Buch können Sie online in unserem
 Shop bestellen.
[Hier zum Shop](#)

2.4 Domänenverwaltung

Beim Erstellen Ihrer Microsoft 365-Umgebung haben Sie sich bereits einen Domännennamen mit der Endung *onmicrosoft.com* ausgesucht, beispielsweise *beispielag.onmicrosoft.com* (siehe Abschnitt 2.1, »Einen Microsoft 365-Mandanten anlegen«). Diese Domäne ist zwar voll funktionsfähig, doch werden Sie diese beispielsweise kaum für E-Mail-Adressen in der Art von *lucy@beispielag.onmicrosoft.com* verwenden wollen.

Sie können eigene Domänen zu Ihrer Microsoft 365-Umgebung hinzufügen, und zwar nicht nur eine, sondern (derzeit) bis zu 900.

Der Prozess zum Hinzufügen einer Domäne ist allerdings in der Praxis nicht ganz unproblematisch und besteht aus mehreren Schritten. Ein wesentlicher Punkt dabei ist, dass Sie beweisen müssen, dass Ihre Domäne auch wirklich unter Ihrer Kontrolle steht. Man spricht hier von einer *Verifikation*. Dazu werden Sie angewiesen, in der DNS-Konfiguration Ihrer Domäne (also typischerweise beim Hoster oder bei der Domänenregistrierungsstelle, über die Sie die Domäne registriert haben) einen bestimmten Eintrag zu hinterlegen. Doch nicht alle Hosters unterstützen dies in der erforderlichen Form. Sollte es hier Probleme geben, müssen Sie die Domäne zunächst zu einem anderen Anbieter umziehen. Der komplette Umzug einer Domäne zu Microsoft ist nicht möglich, sondern es ist nach wie vor ein externer DNS-Anbieter erforderlich.

Tabelle 2.2 erläutert die verschiedenen Typen von DNS-Einträgen, die für Microsoft 365 eine Relevanz haben.

| Typ | Bedeutung | Beschreibung |
|-------|------------------------------|--|
| A | <i>Address Record</i> | Mit einem A-Eintrag weisen Sie einem <i>Hostnamen</i> eine IP-Adresse zu, also beispielsweise <i>remote.beispielag.de</i> zu 84.160.10.122. Einen A-Eintrag benötigen Sie möglicherweise bei der Einrichtung eines <i>Identitätsverbunds</i> (siehe Abschnitt 4.5, »Identitätsverbund«). |
| CNAME | <i>Canonical Name Record</i> | Ein CNAME-Eintrag wird auch <i>Alias</i> genannt. Mit ihm weisen Sie einem Hostnamen einen anderen Hostnamen zu, beispielsweise <i>autodiscover.beispielag.de</i> für <i>autodiscover.outlook.com</i> . CNAME-Einträge benötigen Sie für die <i>Exchange-AutoErmittlung (Autodiscover)</i> und das Mobile Device Management (und gegebenenfalls für Skype for Business, falls dies bei Ihnen noch im Einsatz ist). |

Tabelle 2.2 Typen von DNS-Einträgen

| Typ | Bedeutung | Beschreibung |
|-----|----------------------|--|
| MX | Mail Exchange Record | Mit einem MX-Eintrag wird der Hostname oder die IP-Adresse des E-Mail-Systems für die jeweilige Domäne angegeben. MX-Einträge werden mit einer <i>Priorität</i> konfiguriert. Wenn mehrere MX-Einträge vorhanden sind, wird zuerst versucht, beim E-Mail-System mit der kleinsten Priorität E-Mails auszuliefern. Sollte das nicht möglich sein, werden die anderen E-Mail-Systeme in aufsteigender Priorität kontaktiert. Einen MX-Eintrag benötigen Sie bei Exchange Online für den eingehenden E-Mail-Verkehr. |
| SRV | Service Locator | Mit SRV-Einträgen können Dienste aufgefunden werden. Für Skype for Business müssen Sie SRV-Einträge anlegen. |
| TXT | Text Record | Wie der Name schon sagt, handelt es sich bei TXT-Einträgen um Text. Einen TXT-Eintrag benötigen Sie für die Verifikation einer eigenen Domäne in Ihrem Microsoft 365-Mandanten (oder alternativ einen MX-Eintrag). |

Tabelle 2.2 Typen von DNS-Einträgen (Forts.)

2.4.1 Voraussetzungen an DNS-Anbieter

Damit Sie Ihre eigene Domäne erfolgreich in Microsoft 365 einbinden und alle Dienste uneingeschränkt nutzen können, muss Ihr DNS-Anbieter einige Voraussetzungen erfüllen. Stellen Sie am besten schon vorher sicher, dass diese erfüllt sind, um nicht mitten im Integrationsprozess vor Problemen zu stehen. Achten Sie insbesondere darauf, dass der von Ihnen gebuchte Tarif beim DNS-Anbieter auch die entsprechenden Funktionen enthält; manchmal unterscheiden sich diese je nach Tarif.

In Tabelle 2.3 finden Sie eine Übersicht der Voraussetzungen.

| Dienst | Erforderliche Einträge |
|---------------------|---|
| Domänenverifikation | <ul style="list-style-type: none"> ▶ Anlegen eines TXT-Eintrags für Ihre Domäne (das Anlegen einer Subdomäne ist nicht ausreichend) oder alternativ ▶ Anlegen eines MX-Eintrags |
| Exchange Online | <ul style="list-style-type: none"> ▶ Anlegen eines MX-Eintrags ▶ Anlegen eines TXT-Eintrags ▶ Anlegen eines CNAME-Eintrags |

Tabelle 2.3 Erforderliche Arten von DNS-Einträgen

| Dienst | Erforderliche Einträge |
|---------------------------|--|
| Skype for Business Online | <ul style="list-style-type: none"> ▶ Anlegen von SRV-Einträgen ▶ Anlegen von CNAME-Einträgen |
| Mobilgeräteverwaltung | ▶ Anlegen von CNAME-Einträgen |

Tabelle 2.3 Erforderliche Arten von DNS-Einträgen (Forts.)

2.4.2 Domäne verifizieren

Im Microsoft 365 Admin Center (<https://admin.microsoft.com>) klicken Sie im Bereich EINSTELLUNGEN auf den Abschnitt DOMÄNEN (siehe Abbildung 2.21).

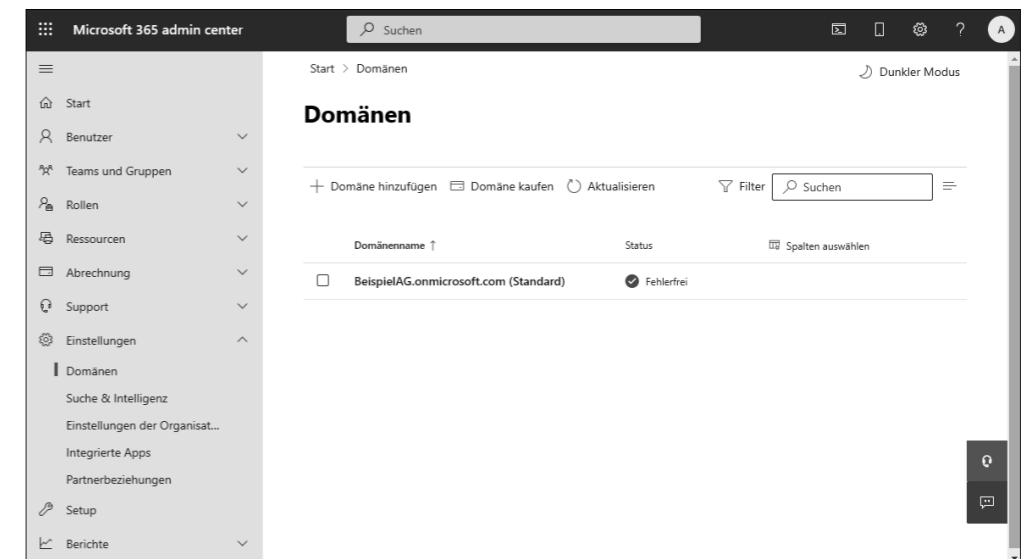


Abbildung 2.21 Domänenverwaltung im Microsoft 365 Admin Center

In der Liste finden Sie alle Domänen, die in der Microsoft 365-Umgebung eingetragen wurden. Die Spalte STATUS gibt Auskunft darüber, ob die jeweilige Domäne bereits erfolgreich verifiziert wurde.

Ihre *onmicrosoft.com*-Domäne kann aus der Liste nicht entfernt werden, wohl aber können Sie über DOMÄNE HINZUFÜGEN den Prozess zur Aufnahme einer eigenen Domäne starten. Dieser Vorgang läuft in folgenden Schritten ab:

1. Domäne hinzufügen
2. Domäne verbinden
3. Fertig stellen

Im Folgenden beschreibe ich jeden dieser Schritte.

Schritt 1: Domäne hinzufügen

Geben Sie zunächst Ihren Domännennamen ein. Abbildung 2.22 zeigt das Fenster dazu.

Weiter geht es mit der Bestätigung des Domänenbesitzes (*Verifikation*), was in der Praxis gerne einmal problematisch wird. Sie erhalten die Anweisung, in der DNS-Konfiguration Ihrer Domäne wahlweise einen TXT-Eintrag, einen MX-Eintrag oder eine vorgegebene Textdatei zur Website der Domäne hinzuzufügen.

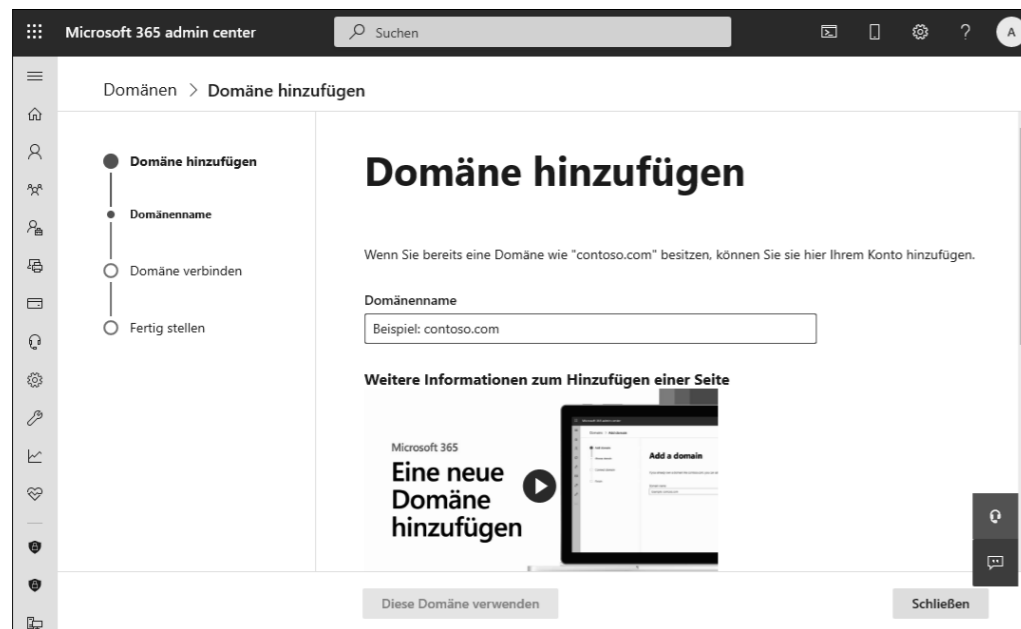


Abbildung 2.22 Domäne angeben

Der TXT-Eintrag für die Überprüfung ist die bevorzugte Methode. Sollte es dabei Probleme geben oder lässt die DNS-Konfiguration Ihres Hosters keine Textdatensätze zu, wählen Sie die MX-Alternative.

Ein Beispiel: Es soll die Domäne *beispielag.de* zur Microsoft 365-Umgebung hinzugefügt werden. Der Textdatensatz wird wie folgt vorgegeben (siehe Abbildung 2.23):

- ▶ **TXT-NAMEN:** @ oder überspringen, wenn vom Anbieter nicht unterstützt
- ▶ **TXT-WERT:** MS=ms74903205

Achten Sie beim Erstellen des Textdatensatzes auf die korrekte Schreibweise mit Groß- und Kleinschreibung. Vermeiden Sie es auch, Leerzeichen mit einzufügen, insbesondere am Ende des Textes. Das passiert gerne, wenn Sie die Zwischenablage verwenden.

- ▶ **TTL:** 3600 oder Standardeinstellung Ihres Anbieters
Nicht bei jedem Anbieter kann die Gültigkeitsdauer vorgegeben werden. In diesem Fall lassen Sie sie einfach weg.

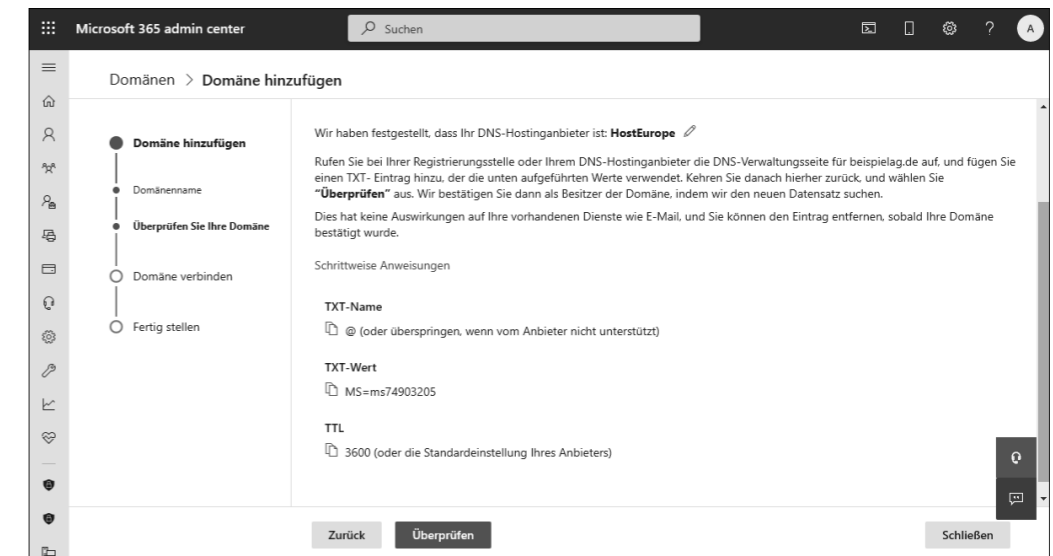


Abbildung 2.23 Domäne überprüfen

Um diesen Vorgang zu verdeutlichen, zeige ich Ihnen anhand des Anbieters *Host Europe* im folgenden Kasten die entsprechende Vorgehensweise.

Domänenverifizierung mit Host Europe

Um den erforderlichen TXT-Eintrag bei Host Europe vorzunehmen, gehen Sie wie folgt vor:

1. Melden Sie sich im Kunden-Informationssystem (KIS) an. Die URL lautet: <https://kis.hosteurope.de>
2. Wechseln Sie zum Bereich **PRODUKTVERWALTUNG**.
3. Wechseln Sie zum Bereich **DOMAINSERVICES**.
4. Wählen Sie im Menü **DOMAIN-ADMINISTRATION** den Punkt **NAMESERVER/ DNS-EINTRÄGE BEARBEITEN**.
5. Klicken Sie auf die Schaltfläche **EDITIEREN** in der Zeile mit der gewünschten Domäne.
6. Gehen Sie in der Tabelle **DNS-EINTRÄGE** ans Ende, und wählen Sie dort in der mittleren Spalte den Eintragstyp **TXT**. In das rechte Textfeld geben Sie genau die Zeichenfolge an, die Sie von Microsoft 365 erhalten haben (MS=ms74903205; siehe Abbildung 2.24).

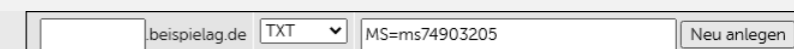


Abbildung 2.24 Neuer TXT-Eintrag

7. Klicken Sie auf NEU ANLEGEN.

8. Warten Sie fünf Minuten.

Bei Host Europe reicht das erfahrungsgemäß aus, bis der neue Eintrag aktiv wird und von Microsoft 365 erkannt werden kann.

Nachdem Sie den erforderlichen Eintrag in der DNS-Konfiguration bei Ihrem Anbieter hinterlegt haben, heißt es warten. Die Konfigurationsänderung muss sich erst in der DNS-Infrastruktur verbreiten. Dieser Vorgang kann zwischen wenigen Minuten und mehreren Tagen dauern. Sie können testweise auf die Schaltfläche ÜBERPRÜFEN klicken. Kann Microsoft 365 die Konfiguration nicht finden, erhalten Sie die Fehlermeldung aus Abbildung 2.25.

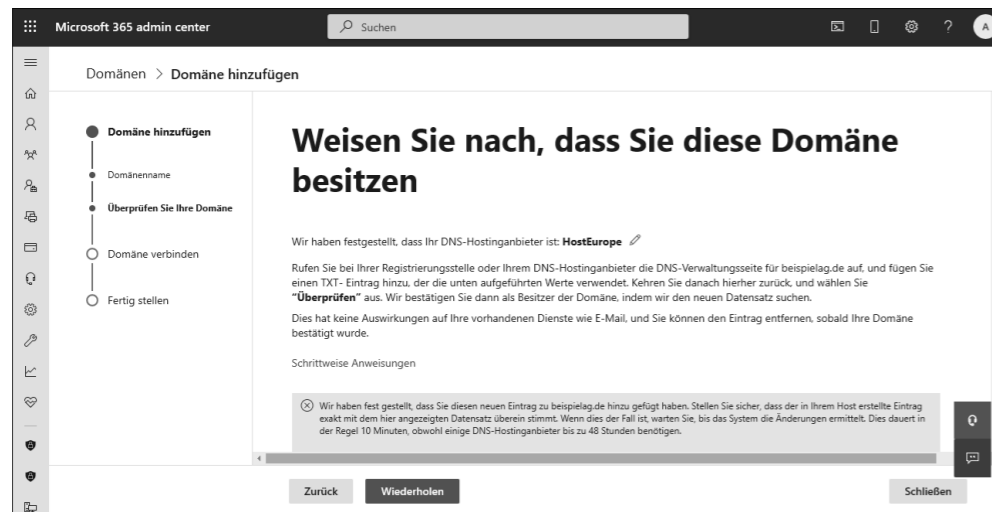


Abbildung 2.25 Fehlgeschlagene Domänenverifizierung

Haben Sie zwischenzeitlich das Microsoft 365 Admin Center verlassen, gelangen Sie über folgenden Weg wieder zurück: Ausgehend von der Domänenliste klicken Sie auf die Domäne und dann auf die Schaltfläche EINRICHTUNG STARTEN.

Will Microsoft 365 Ihre DNS-Konfiguration nicht erkennen, können Sie selbst sicherstellen, dass Ihr DNS-Anbieter die DNS-Einträge korrekt in seiner DNS-Infrastruktur publiziert hat. Auf Websites wie www.heise.de/netze/tools/dns geben Sie Ihren Domännennamen ein und erhalten daraufhin die entsprechenden DNS-Einträge geliefert (siehe Abbildung 2.26). Beispiel: Auf der Website geben Sie unter ABFRAGEART die Option TEXT LOOKUP (TXT RECORD) und unter HOSTNAME ODER ADRESSE den zu überprüfenden Domännennamen ein und klicken dann auf ABSCHICKEN.

Im Abfrageergebnis sehen Sie dann die DNS-Einträge (siehe Abbildung 2.27). Ist dort der erforderliche Eintrag nicht zu sehen, kann Microsoft 365 ihn auch nicht auslesen. Überprüfen Sie in diesem Fall die DNS-Konfiguration.

Abbildung 2.26 Abfrage von DNS-Informationen

Abfrageergebnis für beispielag.de:

| Typ | Daten |
|-----|---|
| TXT | name: beispielag.de txtdata: MS=ms74903205 char_str_list: MS=ms74903205 ttl: 86400 |

Abbildung 2.27 Ergebnis der DNS-Abfrage

Theoretisch könnten Sie statt einer derartigen Website auch das Kommandozeilentool `nslookup` verwenden. Dabei müssen Sie aber beachten, dass dann die Ergebnisse gegebenenfalls nicht vom DNS-Server Ihres Providers beantwortet werden, sondern von Ihrem lokalen DNS-Server. Um mit `nslookup` beispielsweise den DNS-Server von Google mit der IP-Adresse 8.8.8.8 nach den TXT-Einträgen von *beispielag.de* abzufragen, führen Sie den folgenden Befehl aus:

```
nslookup -type=TXT beispielag.de 8.8.8.8
```

Listing 2.1 DNS-Abfrage

Hat das Überprüfen dann tatsächlich geklappt, kann es mit dem nächsten Schritt weitergehen.

Schritt 2: Domäne verbinden

Microsoft 365 benötigt für die Dienste noch eine ganze Reihe weiterer DNS-Einträge. Diese können Sie entweder selbst erstellen, oder aber Sie delegieren diese Aufgabe an Microsoft 365. In letzterem Fall ändern Sie die sogenannten *Nameserver-Einträge* für Ihre Domäne, so dass diese auf das Microsoft-DNS-System zeigen. Diesen Weg gehen wir im weiteren Verlauf nicht, sondern wir legen die DNS-Einträge selbst an. Damit behalten wir die volle Flexibilität.

In Abbildung 2.28 wählen Sie also nicht die Option MEINE ONLINEDIENSTE FÜR MICH EINRICHTEN, sondern die Option FÜGEN SIE IHRE EIGENEN DNS-EINTRÄGE HINZU.

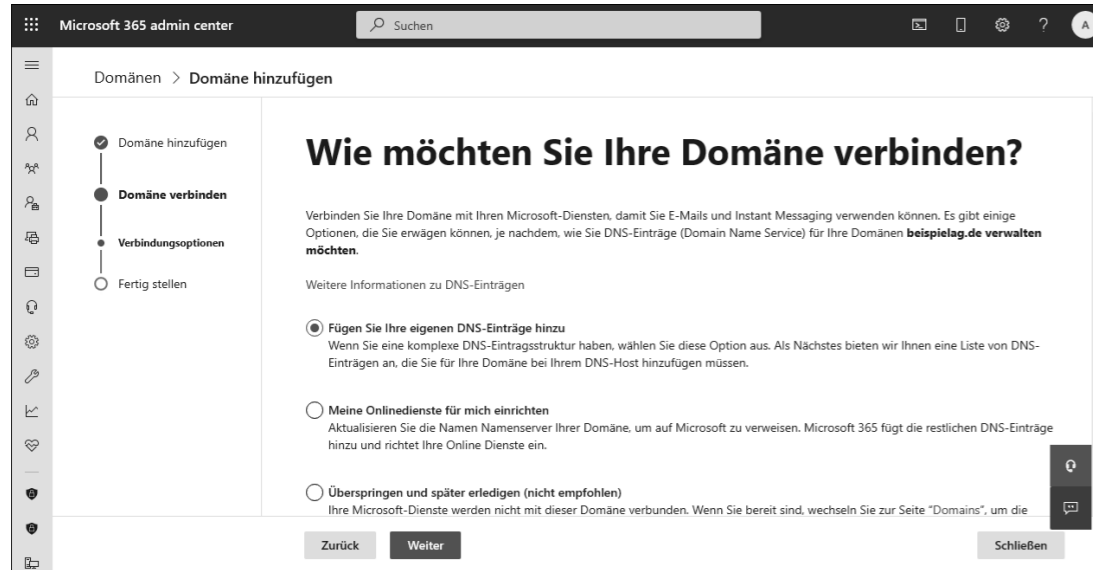


Abbildung 2.28 Onlinedienste einrichten

Schritt 3: DNS-Einstellungen aktualisieren

Der Assistent zeigt Ihnen nun eine lange Liste weiterer DNS-Einträge, die für Microsoft 365 erforderlich sind. Ein Beispiel sehen Sie in Abbildung 2.29.

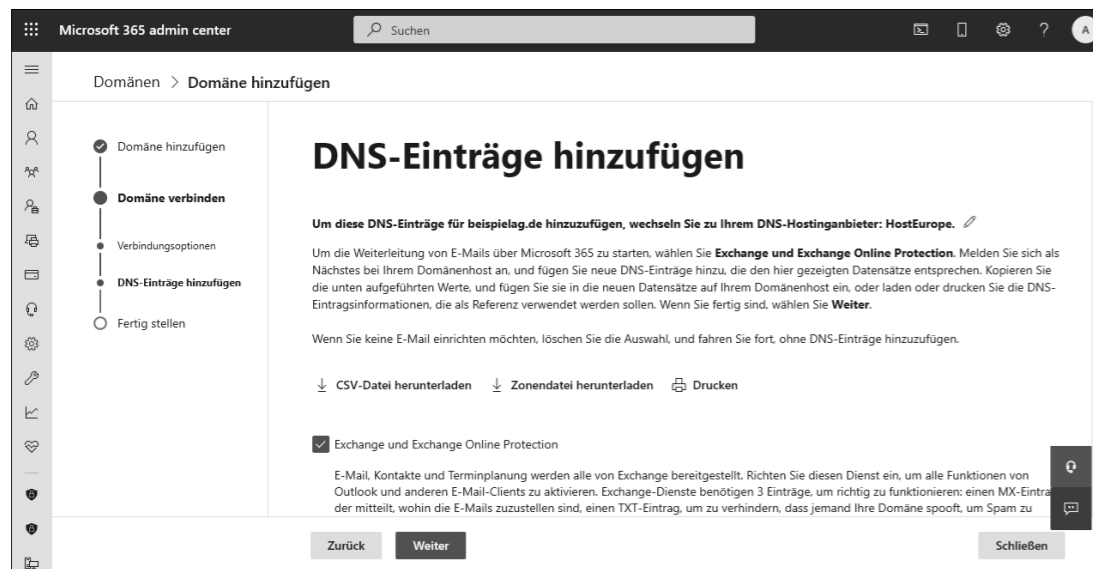


Abbildung 2.29 DNS-Einstellungen

Diese DNS-Einträge sollten Sie erst erstellen bzw. ändern, wenn Sie die eventuell erforderliche Migration von bestehenden Systemen geplant und durchgeführt haben. Müssen Sie beispielsweise zunächst ein vorhandenes E-Mail-System migrieren, ändern Sie nicht sofort den MX-Eintrag, was nämlich zur Folge hätte, dass E-Mails bei Exchange Online und nicht bei Ihrem bestehenden E-Mail-System ausgeliefert würden. Informationen zur E-Mail-Migration finden Sie in Abschnitt 6.9, »Exchange-Migration«.

Vergessen Sie im Zuge der Änderungen der DNS-Einträge bei Ihrem DNS-Anbieter nicht Ihren internen DNS-Server, sofern dort die hinzugefügte Domäne verwaltet wird (Split DNS). Ansonsten bekommen die internen Clients Probleme bei der Verbindung mit den Microsoft 365-Diensten, da sie dafür keine oder eine alte Namensauflösung erhalten. Wichtig ist auch hier wieder, dass Sie die Einträge korrekt vornehmen, um ein einwandfreies Funktionieren der Microsoft 365-Dienste zu ermöglichen. Allerdings gibt es hier keinen Verifikationsprozess wie bei der Aufnahme der Domäne in die Microsoft 365-Umgebung.

Da hier das Vorgehen wieder in hohem Maße von der Konfigurationsoberfläche Ihres Domänenanbieters abhängt, erläutere ich im folgenden Kasten als Beispiel erneut die Vorgehensweise bei Host Europe (andere Anleitungen finden Sie unter <https://docs.microsoft.com/de-de/microsoft-365/admin/setup/add-domain>).

DNS-Einträge bei Host Europe

Beachten Sie zum Anlegen der DNS-Einträge bei Host Europe folgende Punkte:

► MX-Eintrag

Den MX-Eintrag erstellen Sie in der Domänenverwaltung in der Tabelle MX-RECORDS. Die PRIORITÄT setzen Sie nicht auf 0, sondern auf 1 (bei Host Europe ist dies der kleinstmögliche Wert). Das PRÄFIX lassen Sie leer, und unter HOSTNAME/IP geben Sie den Hostnamen an, wie er von Microsoft 365 geliefert wurde. Eine Angabe der Gültigkeitsdauer (TTL) für den Eintrag ist bei Host Europe nach dem Anlegen möglich, aber nicht unbedingt erforderlich. Ein Beispiel sehen Sie in Abbildung 2.30.

| PRIORITÄT | PRÄFIX | HOSTNAME/IP | TTL |
|-----------|--------|--|--|
| 1 | | beispielag-de.mail.protection.outlook.com | Standard (1 Tag - 86400) |
| | | <input type="button" value="Update"/> <input type="button" value="Löschen"/> | <input type="button" value="Speichern"/> |

Abbildung 2.30 MX-Eintrag

► CNAME-Einträge

Den CNAME-Eintrag erstellen Sie in der Tabelle DNS-EINTRÄGE (siehe Abbildung 2.31).

► TXT-Einträge

Den TXT-Eintrag erstellen Sie ebenfalls in der Tabelle DNS-EINTRÄGE. Das Textfeld HOSTNAME lassen Sie dabei leer, und unter HOSTNAME/IP geben Sie den vorgegebenen Text an.



| HOSTNAME | ZEIGT AUF | TTL |
|---|---|------------------------------------|
| beispielag.de ergibt: http://beispielag.de | TXT ▼ v=spf1 include:spf.protection.outlook.com -all | Standard (1 Tag - 86400) Speichern |
| autodiscover.beispielag.de ergibt: http://autodiscover.beispielag.de | CNAME ▼ autodiscover.outlook.com | Standard (1 Tag - 86400) Speichern |
| enterpriseenrollment.beispielag.de ergibt: http://enterpriseenrollment.beispielag.de | CNAME ▼ enterpriseenrollment.manage.microsoft.com | Standard (1 Tag - 86400) Speichern |
| enterpriseregistration.beispielag.de ergibt: http://enterpriseregistration.beispielag.de | CNAME ▼ enterpriseregistration.windows.net | Standard (1 Tag - 86400) Speichern |
| sip.beispielag.de ergibt: http://sip.beispielag.de | CNAME ▼ sipdir.online.lync.com | Standard (1 Tag - 86400) Speichern |
| lyncdiscover.beispielag.de ergibt: http://lyncdiscover.beispielag.de | CNAME ▼ webdir.online.lync.com | Standard (1 Tag - 86400) Speichern |

Abbildung 2.31 CNAME- und TXT-Einträge

► SRV-Einträge

Den SRV-Eintrag erstellen Sie in der Domänenverwaltung in der Tabelle SRV-RECORDS (siehe Abbildung 2.32).

| SERVICE | PROTOKOLL | PRÄFIX (OPTIONAL) | PRIORITÄT | GEWICHT | PORT | HOSTNAME |
|-------------------|-----------|-------------------|-----------|---------|------|-------------------------------------|
| _sip | TLS ▼ | | 100 | 1 | 443 | sipdir.online.lync.c Update Löschen |
| _sipfederationtls | TCP ▼ | | 100 | 1 | 5061 | sipfed.online.lync.c Update Löschen |

Abbildung 2.32 SRV-Einträge

Nachdem Sie die Einträge vorgenommen haben, heißt es wieder warten – von wenigen Sekunden bis zu drei Tagen kann es dauern, bis Ihre Änderungen in der DNS-Infrastruktur veröffentlicht werden. Eine Website wie www.heise.de/netze/tools/dns kann wieder dabei helfen, zu überprüfen, ob die Konfiguration aktiv ist.

Um das Hinzufügen der Domäne abzuschließen, lassen Sie dann noch die DNS-Einstellungen überprüfen.

DNS-Konfigurationen testen

Mit dem Cmdlet `Resolve-DnsName` können Sie DNS-Abfragen direkt über die PowerShell starten. Rufen Sie `Resolve-DnsName -Name beispielag.de -Server 8.8.8.8` auf, um zu überprüfen, ob die DNS-Änderung bereits von den Google-Servern registriert wurde. Auch weitere DNS-Abfragen, beispielsweise nach unterschiedlichen Records, lassen sich mit `Resolve-DnsName` durchführen.

Danach ist es endlich geschafft: Sie können die neue Domäne für die ausgewählten Microsoft 365-Dienste verwenden.

2.4.3 Domäne entfernen

Aus der Domänenliste im Microsoft 365 Admin Center können Sie bereits verifizierte Domänen auch wieder entfernen. Dazu darf die Domäne aber nicht mehr im Gebrauch sein, also beispielsweise weder beim Benutzernamen noch bei E-Mail-Adressen etc. zum Einsatz kommen. Ist sie dennoch in Verwendung, wird automatisch versucht, die Domäne auf die Standarddomäne zu setzen, also die *onmicrosoft.com*-Domäne. Klappt dies in Einzelfällen nicht, erhalten Sie eine Fehlermeldung samt Liste, wo die Domäne noch zum Einsatz kommt.

Benutzernamen und Exchange Online

Wechseln Sie im Microsoft 365 Admin Center im Bereich BENUTZER zum Abschnitt AKTIVE BENUTZER. Überprüfen Sie, ob im Benutzernamen irgendwo die zu löschende Domäne verwendet wird. Sollte dies der Fall sein, öffnen Sie den Benutzer und bearbeiten den Benutzernamen (siehe Abbildung 2.33).

Abbildung 2.33 Domänenänderung bei einem Benutzer

Der Benutzername wird bei Exchange Online-Postfächern automatisch als E-Mail-Adresse verwendet. Sollten Sie in den Postfächern weitere E-Mail-Adressen mit der zu löschenden Domäne angegeben haben, müssen Sie diese auch entfernen.

Die hier vorgestellten Schritte gelten nicht bei Benutzern, die über die automatische Synchronisierung vom Active Directory aus angelegt wurden. Bei solchen Benutzern müssen Sie die Änderung lokal im Active Directory vornehmen, etwa über die Managementkonsole *Active Directory-Benutzer und -Computer*. Zur Active Directory-Synchronisierung lesen Sie mehr in Abschnitt 4.2.1.

Skype for Business Online

Für *Skype for Business Online*-Benutzer wird automatisch eine *SIP-Adresse* vergeben, die grundsätzlich auch beim Ändern der Domäne des Benutzerkontos mit geändert wird.

Standarddomäne

Klicken Sie in der Domänenverwaltung im Microsoft 365 Admin Center auf eine andere Domäne als die, die Sie entfernen wollen. Klicken Sie dann auf die Schaltfläche **ALS STANDARD FESTLEGEN** (siehe Abbildung 2.34).



Abbildung 2.34 Ändern der Standarddomäne

2.5 Benutzerverwaltung

Die Benutzerverwaltung rufen Sie im Microsoft 365 Admin Center über den Punkt **BENUTZER** • **AKTIVE BENUTZER** in der linken Navigationsleiste auf (siehe Abbildung 2.35).

Es hängt allerdings von Ihrer Umgebung ab, ob Sie dort tatsächlich manuell neue Benutzer anlegen können oder ob diese automatisch über eine separate Anwendung, ein *Active Directory-Verzeichnissynchronisierungstool*, angelegt werden. Damit Sie entscheiden können, welche Vorgehensweise für Ihre Umgebung geeignet ist, müssen wir zunächst den Begriff *Microsoft-Online-ID* klären.

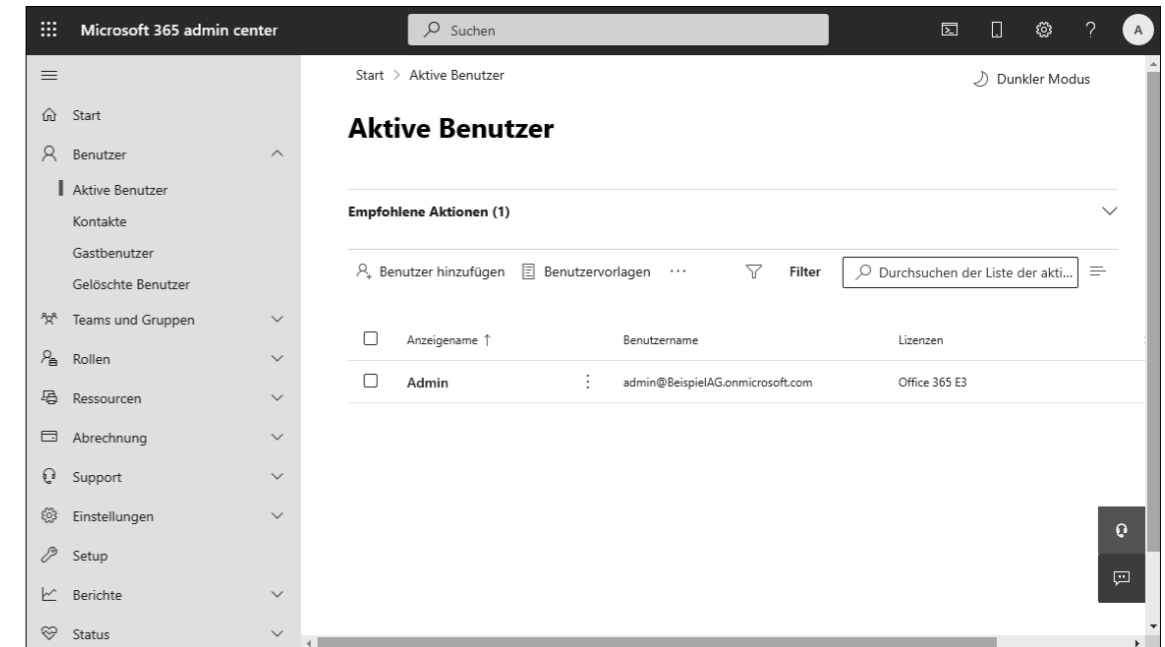


Abbildung 2.35 Benutzerverwaltung

2.5.1 Microsoft-Online-ID

So wie Sie in Ihrer lokalen Umgebung einen *Verzeichnisdienst* einsetzen – nämlich höchstwahrscheinlich das *Active Directory* –, verfügt auch Microsoft 365 über einen eigenen Verzeichnisdienst mit dem Namen *Azure Active Directory (AAD)*. Bei den dort angelegten Benutzerkonten handelt es sich um *Microsoft-Online-IDs*. Diese werden auf Formularen, in die der Anwender seine Zugangsdaten eintragen muss, manchmal auch als *Organisations-, Geschäfts-, Schul- oder Uni-Konto* bezeichnet. Sie benötigen zunächst für jeden Anwender eine solche Microsoft-Online-ID, die Sie dann mit der passenden Lizenz ausstatten und damit entscheiden, welche Microsoft 365-Dienste der Anwender wie nutzen kann.

Die Frage ist nun, ob Sie die IDs selbst anlegen (über das Microsoft 365 Admin Center) oder anlegen lassen (über ein *Active Directory-Verzeichnissynchronisierungstool*). Solch ein Synchronisierungstool wird auf einem Server im lokalen Netzwerk installiert und hat die Aufgabe, regelmäßig neue *Active Directory*-Benutzer im Microsoft 365-Verzeichnisdienst anzulegen, lokal gelöschte ebenfalls zu löschen etc. Das Tool kümmert sich dabei nicht nur um Benutzerkonten, sondern auch um andere Objekttypen wie beispielsweise Gruppen und Kontakte. Werden über ein solches Tool neue Microsoft 365-Benutzer angelegt, müssen Sie diese nachträglich mit einer entsprechenden Lizenz ausstatten, beispielsweise über das Microsoft 365-Portal. Es gibt aber auch andere Wege, etwa automatisiert über die PowerShell. Außerdem benötigt der neue Microsoft 365-Benutzer möglicherweise ein Kennwort. Das Verzeich-

nissynchronisierungstool beherrscht aber auch optional eine Kennwortsynchronisierung, mit der das lokale Kennwort auch zur Anmeldung an Microsoft 365 genutzt werden kann. Der Aufbau ist in Abbildung 2.36 dargestellt.

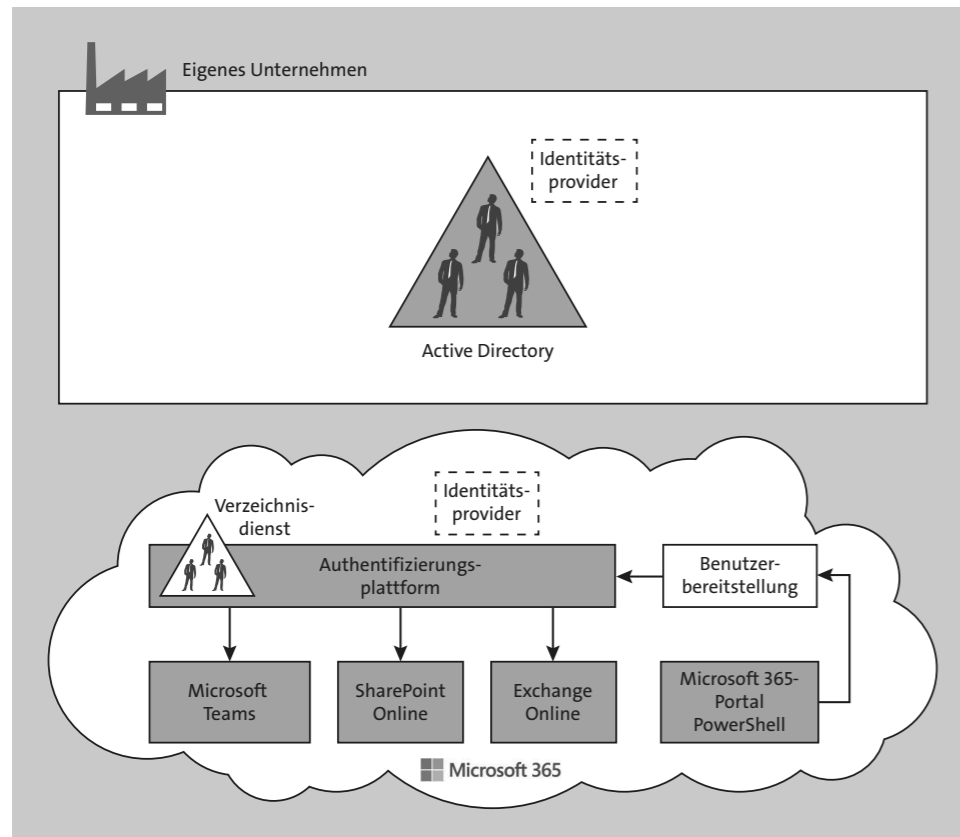


Abbildung 2.36 Verzeichnisdienste im eigenen Unternehmen und in Microsoft 365

In diesem Abschnitt beschreibe ich das manuelle Anlegen von Benutzern über das Microsoft 365-Portal. Die Vorgehensweise mit einem Active Directory-Verzeichnissynchronisierungstool erläutere ich in Abschnitt 4.2.1. Entscheiden Sie sich für die Active Directory-Synchronisierung, verwalten Sie Ihre Microsoft 365-Benutzerkonten nicht über die Microsoft 365-Benutzerverwaltung, sondern über die üblichen Tools Ihres lokalen Active Directorys, beispielsweise über die Managementkonsole *Active Directory-Benutzer und -Computer*.

2.5.2 Benutzer anlegen

Ausgehend von der Benutzerverwaltung im Microsoft 365 Admin Center klicken Sie auf **BENUTZER HINZUFÜGEN** für einen einzelnen Benutzer oder auf **MEHRERE BENUTZER HINZUFÜGEN** für viele Benutzer.

Einzelne Benutzer anlegen

Das Anlegen eines einzelnen Benutzers ist schnell erledigt (siehe Abbildung 2.37).

Abbildung 2.37 Anlegen eines Benutzers

Geben Sie neben einem Vor- und einem Nachnamen einen Anzeigenamen und den gewünschten Benutzernamen an. Die Auswahlliste bei der Domäne des Benutzernamens enthält die Mandantdomäne und gegebenenfalls weitere Domänen, die Sie bereits zu Ihrem Microsoft 365-Mandanten hinzugefügt haben (siehe Abschnitt 2.4, »Domänenverwaltung«).

Soll der Benutzer später zum Administrator werden, müssen Sie den Vor- und den Nachnamen vergeben. Ansonsten sind diese beiden Angaben optional. [«]

Im Standardfall geben Sie das Initialkennwort für den Benutzer vor, Microsoft 365 kann aber auch selbst eines generieren. Außerdem können Sie erzwingen, dass der Benutzer bei der ersten Anmeldung sein Kennwort ändern muss.

Weiter geht es mit den **PRODUKTLIZENZEN**. Hier geben Sie zunächst den Standort des Benutzers an. Abhängig von dieser Auswahl kann es sein, dass einige Funktionen der Microsoft 365-Dienste für diesen Benutzer nur eingeschränkt verfügbar sind. Auch kann es aufgrund von Ausführbeschränkungen sein, dass der Benutzer Microsoft 365 nicht nutzen darf. Beim ersten Anlegen des Benutzers wird der Standort automatisch gewählt. Eine Übersicht der Einschränkungen pro Land finden Sie unter folgender URL:

<https://www.microsoft.com/de-de/microsoft-365/business/microsoft-office-license-restrictions>

Wählen Sie dabei eine oder mehrere Lizenzen, die dem Benutzer zugewiesen werden sollen. Abhängig von den gewählten Lizenzen kann der Anwender dann mit den Microsoft 365-Diensten arbeiten. Wählen Sie beispielsweise eine Exchange Online-Lizenz, wird daraufhin automatisch ein Postfach für den Benutzer angelegt.

Bei den **OPTIONALEN EINSTELLUNGEN** geben Sie unter **PROFILINFORMATIONEN** weitere Daten ein, beispielsweise die Adressdaten. In diesem Abschnitt finden Sie aber auch die **ROLLEN**. Hier können Sie den Benutzer zu einem Administrator machen, um es ihm zu ermöglichen, verschiedene Verwaltungsaufgaben in Ihrer Microsoft 365-Umgebung vorzunehmen. Tabelle 2.4 listet die grundlegenden Rollen auf. Neben diesen gibt es jedoch noch eine ganze Reihe weitere dienstspezifische Rollen. Auf diese gehe ich dann in den zugehörigen Kapiteln ein.

| Rolle | Beschreibung |
|-----------------------------|--|
| Benutzeradministrator | Setzt Benutzerkennwörter zurück, erstellt und verwaltet Benutzer und Gruppen, einschließlich Filter, verwaltet Serviceanfragen und überwacht den Dienststatus. |
| Dienst-Supportadministrator | Erstellt Serviceanfragen und überwacht den Dienststatus. |
| Exchange-Administrator | Hat Vollzugriff auf Exchange Online, erstellt und verwaltet Gruppen, verwaltet Serviceanfragen und überwacht den Dienststatus. |
| Globaler Administrator | Verfügt über uneingeschränkten Zugriff auf alle Verwaltungsfunktionen und die meisten Daten in allen Admin Centern. |
| Globaler Leser | Kann alle administrativen Funktionen und Einstellungen in allen Admin Centern anzeigen. |
| Helpdesk-Administrator | Setzt Kennwörter zurück, verwaltet Serviceanfragen und überwacht den Dienststatus. |
| SharePoint-Administrator | Hat Vollzugriff auf SharePoint Online, verwaltet Microsoft 365-Gruppen und Serviceanfragen und überwacht den Dienststatus. |
| Teams-Administrator | Hat Vollzugriff auf Microsoft Teams, verwaltet Microsoft 365-Gruppen und Serviceanfragen und überwacht den Dienststatus. |

Tabelle 2.4 Administratorrollen

Empfehlungen zur Konfiguration von Administrator-Benutzerkonten

Benutzerkonten, denen Sie eine administrative Rolle zugewiesen haben, können in Ihrem Microsoft 365-Mandanten recht weitgehende Berechtigungen einsetzen. Entsprechend sorgfältig sollten Sie bei der Konfiguration dieser Benutzerkonten sein, sodass diese möglichst nicht missbraucht werden. In der Praxis haben sich dabei folgende Punkte bewährt:

- ▶ **Anzahl**
Auch Administratoren sind manchmal nicht verfügbar. Damit dann aber dennoch dringende Konfigurationen durchgeführt werden können, sollte nicht nur eine einzelne Person über ein administratives Benutzerkonto verfügen.
- ▶ **Kein produktives Benutzerkonto**
Diese Empfehlung gilt nicht nur für Microsoft 365: Ein Benutzerkonto, das der Anwender für seine tägliche Arbeit verwendet, sollte keine administrativen Berechtigungen erhalten. Legen Sie für administrative Aufgaben ein separates und personalisiertes Benutzerkonto an. Somit sind Alltag und administrative Aufgaben klar voneinander getrennt.
- ▶ **Benutzername**
Der Benutzername von administrativen Benutzern sollte auf der Mandantdomäne (*on-microsoft.com*) enden. Damit sind Administrator-Benutzerkonten klar von produktiven Benutzerkonten getrennt. Außerdem können Sie solche Benutzer auch noch am Mandanten anmelden, wenn beispielsweise ein Domänenverbund auf Basis von AD FS nicht mehr funktionsfähig ist (siehe Abschnitt 4.5, »Identitätsverbund«). Die Gefahr, dass sich Administratoren damit selbst ausschließen, ist somit geringer.
- ▶ **Kennwort**
Verwenden Sie ein langes und komplexes Kennwort. Verwenden Sie das Kennwort bei keinem anderen Benutzerkonto.
- ▶ **Alternative E-Mail-Adresse und Mobilfunknummer**
Administratoren können ihr Kennwort selbst zurücksetzen. Dies setzt aber voraus, dass eine alternative E-Mail-Adresse sowie eine Mobilfunknummer beim Benutzerkonto hinterlegt wurden. Lesen Sie hierzu Abschnitt 2.9.2, »Administratorkennwort zurücksetzen«.
- ▶ **Mehrstufige Authentifizierung**
Um den Anmeldeprozess von administrativen Benutzern sicherzustellen, sollten Sie für diese die mehrstufige Authentifizierung aktivieren. Damit reicht es nicht mehr aus, beim Anmelden nur das Kennwort anzugeben. Darüber hinaus ist ein zweiter Schritt erforderlich, wie die Bestätigung per App, Anruf oder SMS. Wie die mehrstufige Authentifizierung aktiviert wird, lesen Sie in Abschnitt 12.2.1, »Mehrstufige Authentifizierung«.
- ▶ **Privileged Identity Management (PIM)**
Speziell für die Benutzerkonten von Administratoren sollten Sie die Verwendung des Privileged Identity Managements (PIM) erwägen. Mit PIM haben auch Benutzerkonten, denen Sie administrative Rechte zugewiesen haben, ständig die Möglichkeit, diese Rechte auch auszuüben. Selbst ein globaler Administrator müsste zunächst diese Rechte anfragen, gegebenenfalls eine Genehmigung erhalten und kann erst danach die Rechte auch

umsetzen – und das auch nur für einen konfigurierbaren Zeitraum. Dieser Prozess wird dabei auch protokolliert, sodass Sie eine Liste erhalten, wann welcher Benutzer zu welchem Zweck administrative Rechte angefordert hat. Mehr dazu lesen Sie in Abschnitt 12.2.4, »Privileged Identities«.

Unmittelbar nach dem Anlegen kann sich der Benutzer an Microsoft 365 anmelden und die lizenzierten Dienste nutzen.

Mehrere Benutzer auf einmal anlegen

Ist Ihnen das Durchlaufen der einzelnen Schritte beim Anlegen mehrerer Benutzer zu aufwendig, können Sie über den Befehl MEHRERE BENUTZER HINZUFÜGEN auch viele Benutzer auf einmal anlegen lassen (siehe Abbildung 2.38).

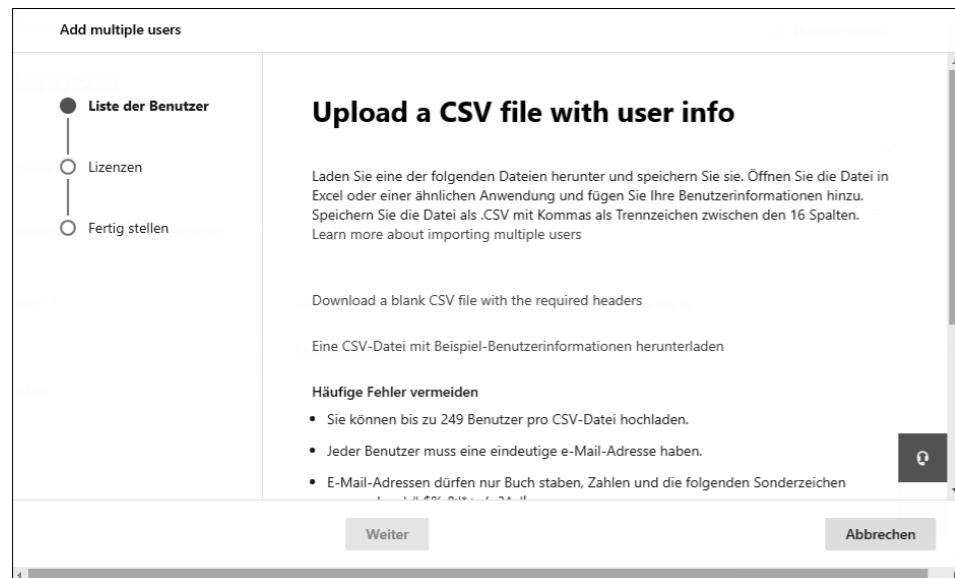


Abbildung 2.38 Massenanlegen von Benutzern

Die Grundlage ist dabei eine *CSV-Datei* (*CSV = Comma-separated Values*), die Sie vorher in folgendem Format anlegen müssen:

Benutzername, Vorname, Nachname, Anzeigename, Position, Abteilung, Büronummer, Telefon (geschäftlich), Mobiltelefon, Faxnummer, Adresse, Ort, Bundesland/ Kanton, Postleitzahl, Land oder Region

Listing 2.2 Aufbau einer CSV-Datei

Nachdem Sie die CSV-Datei hochgeladen haben, wird der Inhalt analysiert. Dabei wird beispielsweise überprüft, ob Sie beim Anmeldenamen nur Domänen angegeben haben, die Be-

standteil Ihrer Microsoft 365-Umgebung sind. Ist die Datei in Ordnung, machen Sie dann die Angaben wie beim Anlegen eines einzelnen Benutzers, nur dass diese dann für alle neuen Benutzer aus der CSV-Datei gelten.

Benutzer können Sie auch automatisiert mithilfe der PowerShell anlegen und dabei auch eigene Kennwörter vergeben. Wie das geht, lesen Sie in Abschnitt 2.5.2, »Benutzer anlegen«.



2.5.3 Benutzer verwalten

Über die Benutzerverwaltung können Sie nicht nur neue Benutzer anlegen, sondern auch bestehende verwalten. Klicken Sie dazu einfach auf den jeweiligen Anzeigenamen des Benutzers. Dort finden Sie die in Abbildung 2.39 gezeigten Einstellungen.

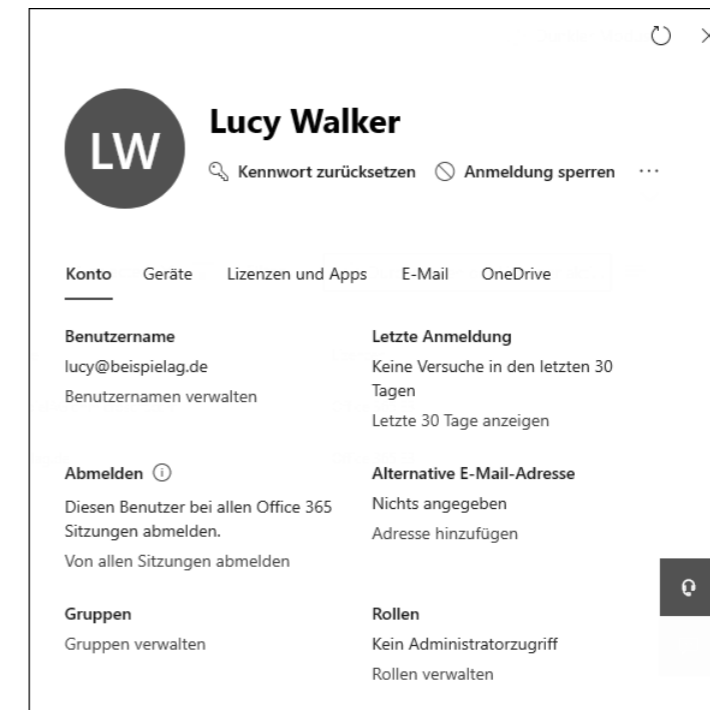


Abbildung 2.39 Benutzereinstellungen verwalten

► Abschnitt KONTO

- BENUTZERNAME
- ALTERNATIVE E-MAIL-ADRESSE: gegebenenfalls weitere E-Mail-Adressen
- GRUPPEN: Hier können Sie den Benutzer als Mitglied diverser Gruppen aufnehmen (siehe Abbildung 2.40). Als Gruppe zählen hier Microsoft 365-Gruppen, E-Mail-Verteilergruppen und Sicherheitsgruppen. Mehr dazu lesen Sie in Abschnitt 6.5.3, »Gruppen und Listen«.

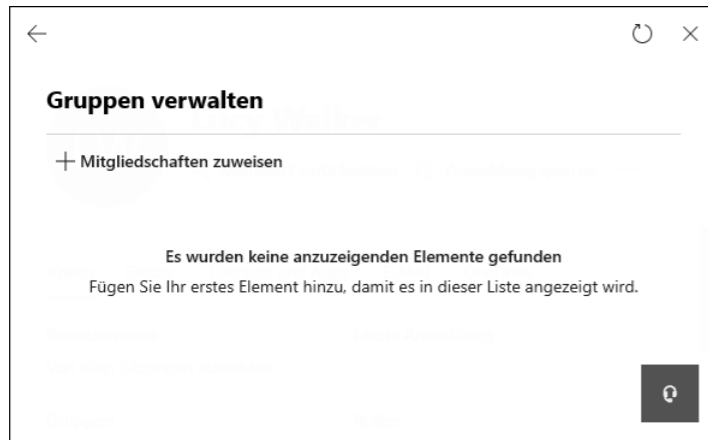


Abbildung 2.40 Gruppenmitgliedschaft verwalten

- ROLLEN: Hier geben Sie dem Benutzer administrative Rechte oder entziehen sie ihm. Dazu verwalten Sie die Rollen eines Benutzers (siehe Abbildung 2.41).

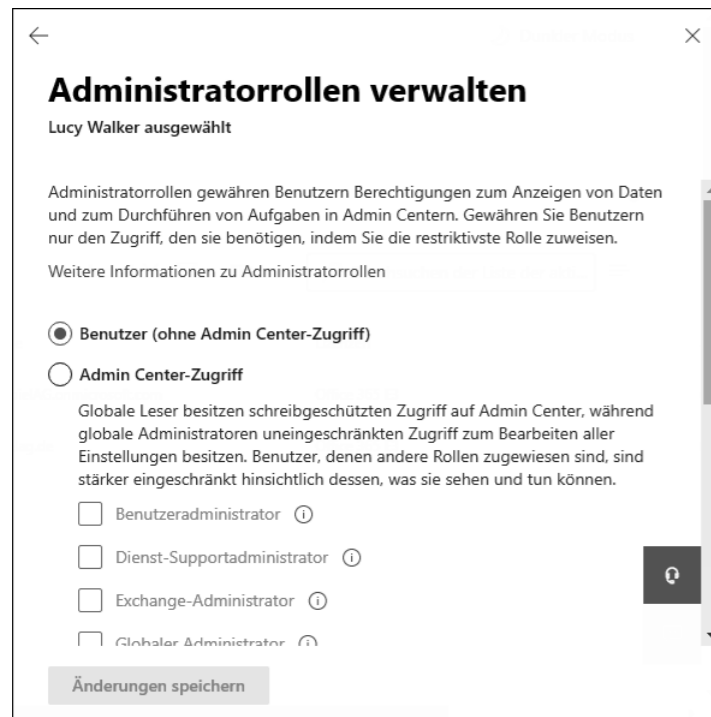


Abbildung 2.41 Benutzerrollen bearbeiten

Mehr dazu lesen Sie in Abschnitt 2.5.2, »Benutzer anlegen«. Wählen Sie eine Administratorrolle, müssen Sie auch eine alternative E-Mail-Adresse angeben, über die der Benutzer

für den Fall, dass er das Kennwort vergessen haben sollte, ein neues erstellen kann. Dazu muss im Benutzerkonto auch eine Mobilfunknummer eingetragen werden. Mehr dazu lesen Sie in Abschnitt 2.9.2, »Administratorkennwort zurücksetzen«.

- KONTAKTINFORMATIONEN: Dieser Bereich enthält Angaben zum Benutzer wie Rufnummern und die Adresse.
- OFFICE-AKTIVIERUNGEN: Hier sehen Sie eine Liste aller Windows- und macOS-Desktops, auf denen der Benutzer das Office-Paket installiert und aktiviert hat (siehe Abbildung 2.42). Bei Bedarf können Sie hier auch die Aktivierung eines Geräts wieder zurücknehmen.
- MEHRSTUFIGE AUTHENTIFIZIERUNG: Soll der Benutzer bei der Anmeldung neben seinem Kennwort einen zweiten Faktor angeben, aktivieren Sie die mehrstufige Authentifizierung (siehe Abschnitt 12.2.1, »Mehrstufige Authentifizierung«).



Abbildung 2.42 Office-Installationen

- ▶ Abschnitt GERÄTE
Dieser Abschnitt gehört zur Geräteverwaltung über Microsoft Intune. Lesen Sie hierzu Abschnitt 14.3.
- ▶ Abschnitt LIZENZEN UND APPS
Bevor Sie einem Benutzer eine Lizenz zuweisen können, muss ein ORT ausgewählt sein. Damit ist der primäre Aufenthaltsort des Anwenders gemeint (siehe Abbildung 2.43). Weisen Sie dem Benutzer eine Lizenz zu. Verfügen Sie über Lizenzpakete, die mehrere Einzellicenzen umfassen (beispielsweise E3), können Sie an dieser Stelle auch einzelne Bestand-

teile aus dem Paket herausnehmen (beispielsweise das Office-Paket, wenn Sie dieses anderweitig lizenzieren oder nicht benötigen). Nicht zugewiesene Bestandteile eines Lizenzpakets können Sie aber nicht einem anderen Benutzer zuweisen.

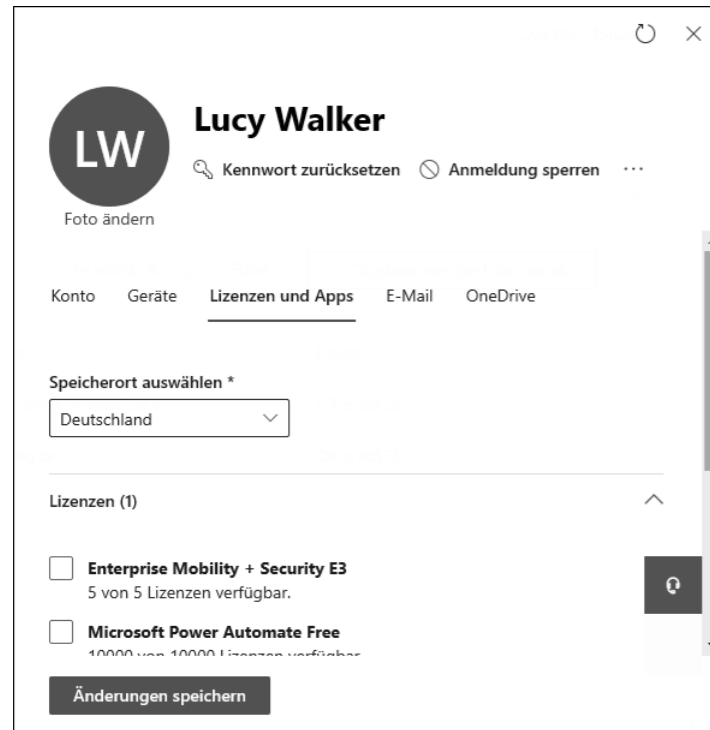


Abbildung 2.43 Verwaltung der Produktlizenzen

► Abschnitt E-MAIL

Die Einstellungen in diesem Bereich finden Sie auch im Exchange Admin Center. Voraussetzung wird hierbei, dass der Benutzer über eine Lizenz für Exchange Online verfügt (siehe Abbildung 2.44).

- **POSTFACHBERECHTIGUNGEN:** Einstellen können Sie hier Leseberechtigungen sowie die Rechte *Senden als* und *Senden im Auftrag von*.
- **IN GLOBALER ADRESSENLISTE ANZEIGEN:** Auswahl, ob der Benutzer in der allgemeinen Adressliste (beispielsweise bei der Auswahl eines E-Mail-Empfängers) angezeigt werden soll.
- **AUTOMATISCHE ANTWORTEN:** Die automatischen Antworten gehören zum Abwesenheitsassistenten, mit dem die Absender von E-Mails, die an diesen Benutzer eine E-Mail schicken, benachrichtigt werden (beispielsweise während des Urlaubs).

- **E-MAIL-APPS:** Hier legen Sie fest, welche der folgenden Apps und Protokolle ein Benutzer verwenden kann, um auf sein Postfach zuzugreifen: Outlook im Web, Outlook-Desktop (MAPI), Exchange-Webdienste, Mobil (Exchange ActiveSync), IMAP, POP.
- **E-MAIL-WEITERLEITUNG:** Hier können Sie einstellen, ob und an welche E-Mail-Adresse alle E-Mails weitergeleitet werden, die an diesen Benutzer geschickt werden.
- **WEITERE AKTIONEN:** Führt Sie zu den Postfacheinstellungen im Exchange Admin Center.

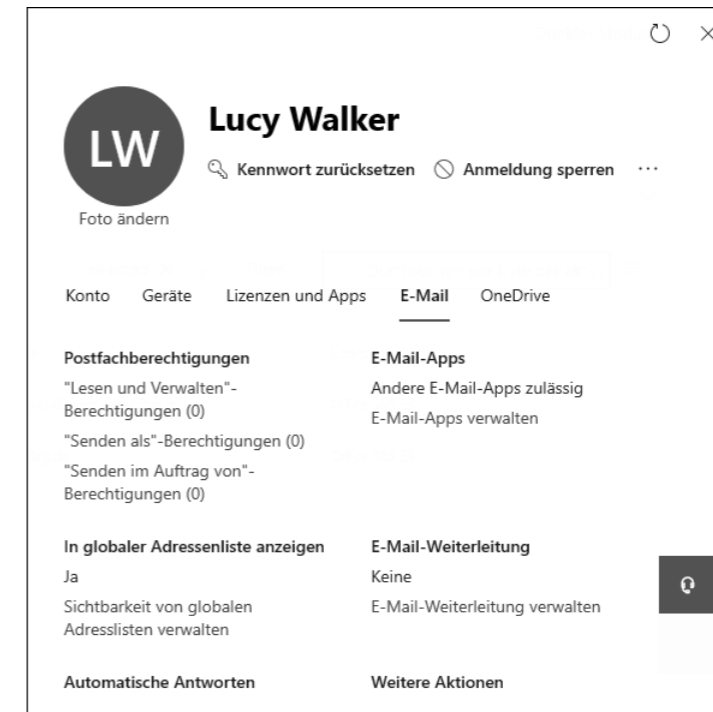


Abbildung 2.44 E-Mail-Einstellungen

► Abschnitt ONEDRIVE

Diese Einstellungen setzen voraus, dass Sie dem Benutzer eine Lizenz für OneDrive for Business zugewiesen haben (siehe Abbildung 2.45).

- **ZUGRIFF AUF DATEIEN ERHALTEN:** Von hier aus können Sie das OneDrive des Benutzers aufrufen. Dort sehen Sie allerdings nur die Inhalte, die der Benutzer für Sie freigegeben hat. Benötigen Sie Zugriff auf den kompletten Inhalt, lesen Sie in Abschnitt 8.7.10, »Administrativer Zugriff auf OneDrive-Inhalte«, nach.
- **VERWENDETER SPEICHER:** Zeigt Ihnen den Füllstand des OneDrives an.

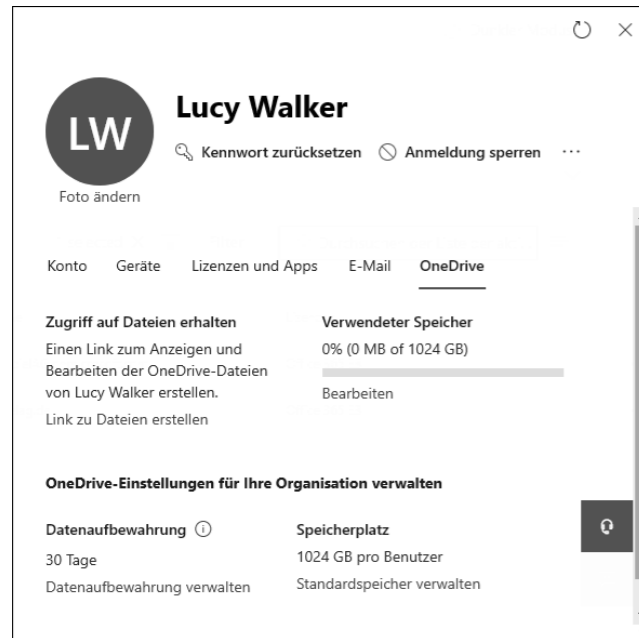


Abbildung 2.45 OneDrive-Einstellungen

Um Ihnen die Verwaltung von vielen Benutzerkonten zu vereinfachen, stehen verschiedene Filter zur Auswahl bereit, beispielsweise **BENUTZER MIT FEHLERN** und **NICHT LIZENZIERTER BENUTZER** (siehe Abbildung 2.46).

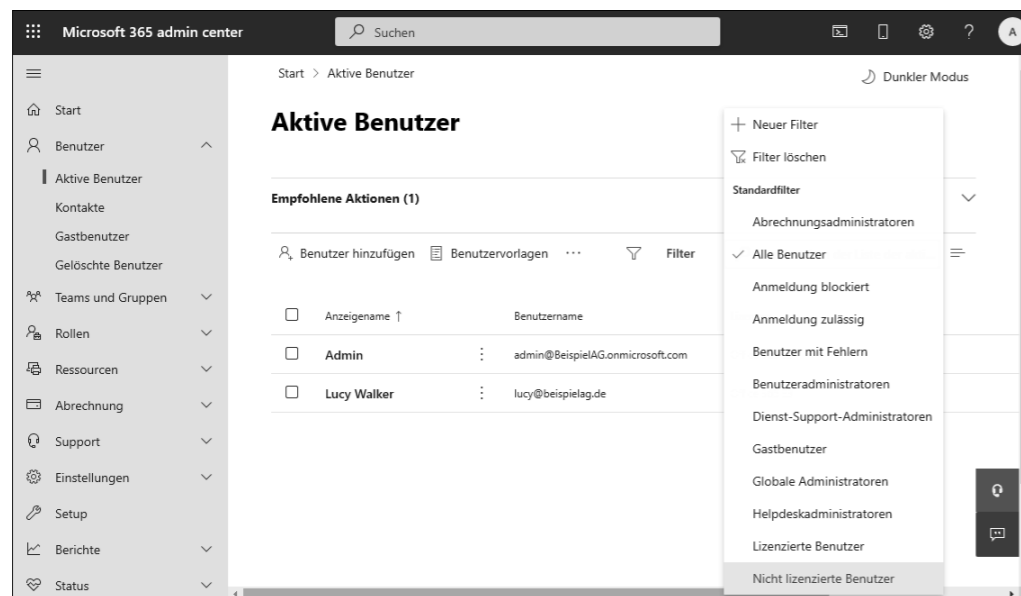


Abbildung 2.46 Auswahl eines Filters

Sie können auch eigene Ansichten anlegen und dabei etwa auf die optionalen Eigenschaften der Benutzer zugreifen, beispielsweise auf die Adresse. Eigene Filter können Sie darüber hinaus auch selbst anlegen.

2.5.4 Gelöschte Benutzer wiederherstellen

Innerhalb von 30 Tagen lassen sich gelöschte Benutzer wiederherstellen. Dazu wechseln Sie im Bereich **BENUTZER** zum Abschnitt **GELÖSCHTE BENUTZER** (siehe Abbildung 2.47).

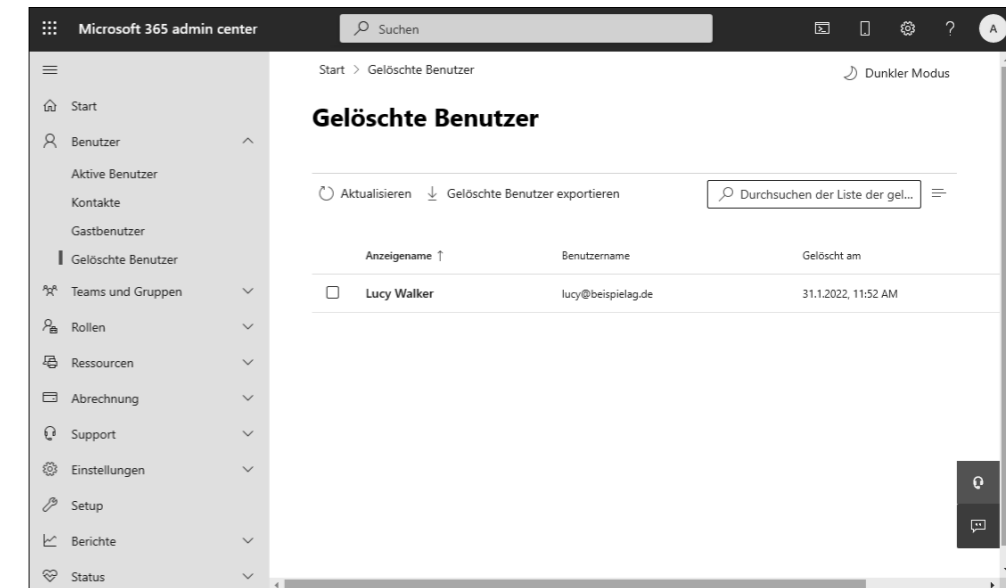


Abbildung 2.47 Verwaltung gelöschter Benutzer

Hatte der gelöschte Benutzer ein Postfach, wird auch dieses wiederhergestellt. Beachten Sie, dass ein gelöscht Benutzerkonto nach 30 Tagen nicht mehr wiederhergestellt werden kann – auch nicht über eine Anfrage an den Microsoft-Kundendienst.

Die Wiederherstellung können Sie auch über die PowerShell automatisieren. Außerdem gibt es dort eine Möglichkeit, einen gelöschten Benutzer schon vor Ablauf der 30 Tage dauerhaft zu entfernen. Lesen Sie hierzu Abschnitt 3.14.6, »Benutzer löschen und wiederherstellen«.

2.5.5 Kennwortablaufrichtlinie

In der Standardkonfiguration laufen bei Microsoft 365-Benutzerkonten die Kennwörter regelmäßig nach 90 Tagen ab. Allerdings gibt es davon auch Ausnahmen:

- Sie haben über das Microsoft 365 Admin Center oder die PowerShell das Ablauf des Kennworts für bestimmte Benutzerkonten deaktiviert (siehe Abschnitt 3.14.4, »Benutzer anlegen«).

- ▶ Sie verwenden die Kennwortsynchronisierung eines Active Directory-Synchronisierungstools. In diesem Fall gelten die Kennwortrichtlinien Ihres lokalen Active Directorys und nicht die von Microsoft 365 (siehe Abschnitt 4.2.1, »Verzeichnissynchronisierung«).
- ▶ Sie verwenden einen Identitätsverbund oder die Passthrough-Authentifizierung. Auch in diesem Fall gelten die Kennwortrichtlinien Ihres lokalen Active Directorys (siehe Abschnitt 4.2.3, »Passthrough-Authentifizierung (PTA)«, und Abschnitt 4.5, »Identitätsverbund«).

Zur Anpassung der Kennwortablafrichtlinie für Microsoft 365-Benutzerkonten existieren drei Einstellungen:

- ▶ Die Kennwörter von Benutzern laufen nie ab.
- ▶ Die Anzahl der Tage, bis ein Kennwort abläuft: Diese Anzahl kann zwischen 14 und 730 liegen. Der Standardwert beträgt 90 Tage.
- ▶ Die Anzahl der Tage, bis Benutzer über das Ablauf des Kennworts benachrichtigt werden: Hier gilt als Standard 14 Tage. Der Zeitraum muss außerdem kleiner gewählt werden als der Zeitraum bis zum Ablauf des Kennworts.

Diese Optionen können Sie über das Microsoft 365 Admin Center bearbeiten. Öffnen Sie dazu im Bereich EINSTELLUNGEN den Abschnitt EINSTELLUNGEN DER ORGANISATION. Wechseln Sie dann zur Registerkarte SICHERHEIT UND DATENSCHUTZ. Klicken Sie dort bei der KENNWORTABLAUFRICHTLINIE auf die Schaltfläche BEARBEITEN, um auf das Formular aus Abbildung 2.48 zu gelangen.

Kennwortablafrichtlinie

Wählen Sie die Anzahl der Tage aus, bis das Kennwort eines Benutzers abläuft, sowie die Anzahl der Tage, bis Sie über einen bevorstehenden Kennwortablauf benachrichtigt werden. Diese Richtlinie gilt für alle in Ihrer Organisation.

Weitere Informationen zu Empfehlungen für Kennwortrichtlinien

Kennwörter festlegen, sodass sie nach einer Anzahl von Tagen ablaufen

Tage bis zum Ablauf der Kennwörter *

90

Tage, bis ein Benutzer über den Ablauf informiert wird *

14

Speichern

Abbildung 2.48 Kennwortablafrichtlinie

Den PowerShell-Ansatz zur Anpassung der Kennwortablafrichtlinie finden Sie in Abschnitt 3.14.4, »Benutzer anlegen«.

2.5.6 Sicherheitsgruppen

Sicherheitsgruppen sind kein neues Konzept, sondern beispielsweise auch im Active Directory enthalten. Mit ihnen gruppieren Sie Benutzerkonten, um sie beispielsweise als Grundlagen von Berechtigungen in SharePoint Online-Umgebungen einzusetzen.

Die Sicherheitsgruppen verwalten Sie im Microsoft 365 Admin Center im Bereich TEAMS UND GRUPPEN unter AKTIVE TEAMS UND GRUPPEN (siehe Abbildung 2.49).

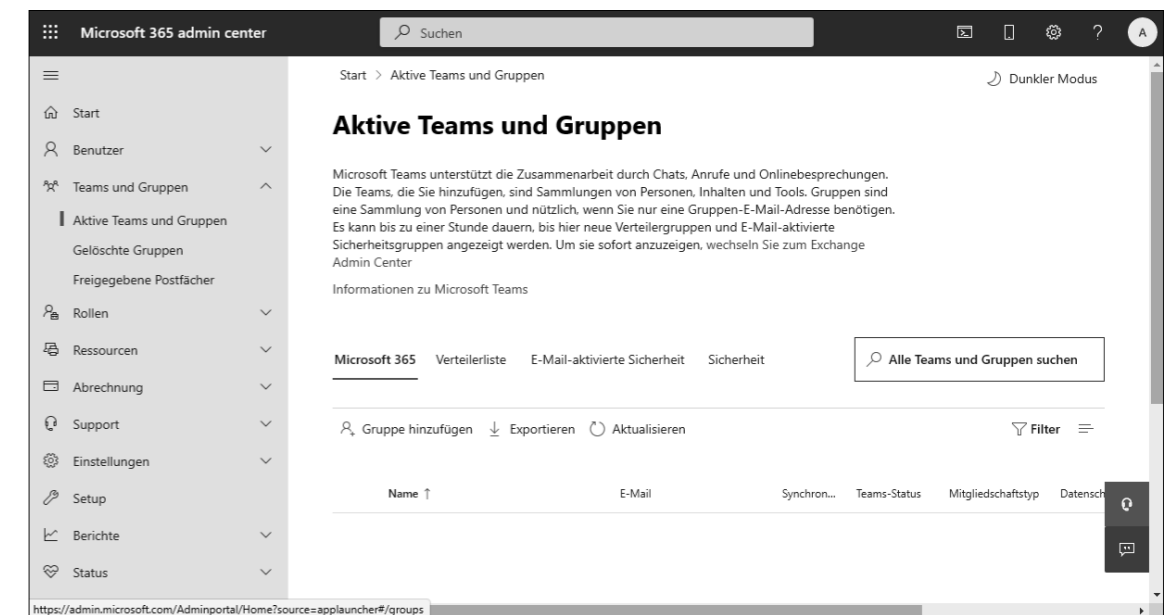


Abbildung 2.49 Gruppenverwaltung

Wie auch Benutzerkonten können Sie direkt im Admin Center weitere Sicherheitsgruppen anlegen oder dies über das Active Directory-Verzeichnissynchronisierungstool automatisch erledigen lassen (siehe Abschnitt 4.2.1, »Verzeichnissynchronisierung«).

Beim manuellen Anlegen gehen Sie wie folgt vor:

1. Klicken Sie auf GRUPPE HINZUFÜGEN (siehe Abbildung 2.50).
2. Wählen Sie einen Gruppentyp. Zur Auswahl stehen MICROSOFT 365, VERTEILUNG, E-MAIL-AKTIVIERTE SICHERHEIT und SICHERHEIT. Die Unterschiede zwischen den Typen lernen Sie in Abschnitt 6.5.3, »Gruppen und Listen«, kennen.
3. Geben Sie einen NAMEN für die neue Gruppe an und weitere Parameter, die sich je nach Typ unterscheiden.

4. Legen Sie die Gruppe mit HINZUFÜGEN an.
5. Öffnen Sie die Gruppe, und fügen Sie Mitglieder hinzu.

Wählen Sie mit einem Klick auf MITGLIEDER BEARBEITEN die gewünschten Gruppenmitglieder aus.

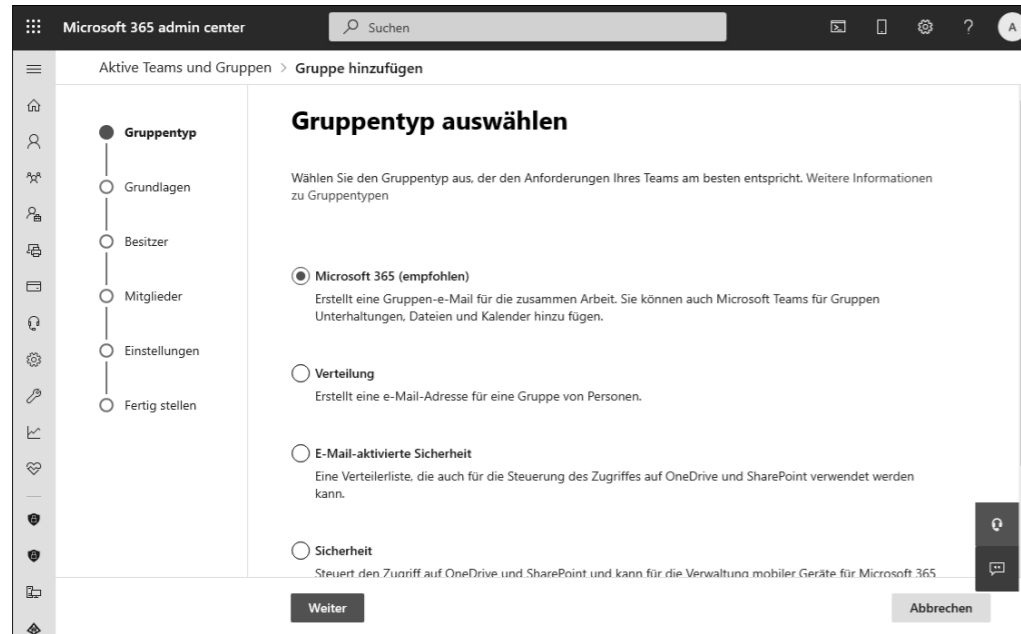


Abbildung 2.50 Neue Gruppe anlegen

2.6 Berichte

Als Administrator haben Sie im Microsoft 365 Admin Center Zugriff auf eine ganze Reihe verschiedener Berichte, die Ihnen helfen, den Überblick über Ihren Microsoft 365-Mandanten und die Aktivitäten Ihrer Anwender zu behalten. Die verschiedenen Berichte erreichen Sie über den Bereich BERICHTE (ein Beispiel sehen Sie in Abbildung 2.51).



Sind Sie insbesondere an detaillierten Statistiken zur Nutzung der Microsoft 365-Dienste interessiert, sollten Sie sich das *Microsoft 365 Adoption Content Pack für Power BI* (siehe Abschnitt 15.2.1) näher ansehen. Eine Dokumentation dazu finden Sie hier:

<https://docs.microsoft.com/de-de/office365/admin/usage-analytics/usage-analytics>

6.9 Exchange-Migration

Historisch gesehen gibt es für Exchange Online einige integrierte Migrationsverfahren, mit denen Sie bestehende Exchange-Postfächer migrieren können, allen voran die Übernahmemigration und die mehrstufige Migration. Beide haben das Ziel, innerhalb eines überschaubaren Zeitraums die lokalen Postfächer zu Exchange Online zu überführen, sodass die lokale Exchange-Umgebung abgeschaltet werden kann.

Inzwischen sind diese beiden Migrationsmethoden in der Praxis nur noch selten anwendbar: Die Übernahmemigration eignet sich nur für eher kleine Exchange-Umgebungen mit maximal 2.000 Postfächern. Allerdings sollten die Postfächer aus Ausfallgründen in einem sehr kurzen Zeitraum migriert werden, beispielsweise über das Wochenende. Außerdem ist die Übernahmemigration nur dann möglich, sofern eine der Exchange-Versionen ab 2003 zum Einsatz kommt. Für viele Unternehmen ist das schon allein aufgrund der zu übertragenden Gesamtkapazität und der verfügbaren Internetbandbreite keine Option.

Solche Unternehmen könnten theoretisch zur mehrstufigen Migration greifen, bei der die Migration der Postfächer in handlichen Häppchen vorgenommen wird und damit auch ein Migrationszeitraum von einigen Wochen bis wenigen Monaten möglich wäre. Doch hat die mehrstufige Migration ein anderes Problem: Sie ist nur mit den inzwischen in die Jahre gekommenen Exchange-Versionen 2003 und 2007 möglich, nicht aber mit den neueren Versionen.

Daneben haben die Übernahmemigration und die mehrstufige Migration auch noch einen weiteren großen Nachteil: Die Outlook-Profile müssen nach der Migration auf den Clients neu angelegt werden. Das bedeutet zusätzlichen Aufwand bei der Einrichtung; hinzu kommt, dass sich die Clients den Postfachinhalt erneut herunterladen.

Vielen Unternehmen blieb daher nichts anderes übrig, als entweder zu einem Tool eines Drittherstellers zu greifen oder eine Exchange-Hybridkonfiguration aufzubauen (siehe Abschnitt 6.10). Eine solche Hybridkonfiguration ist eigentlich dafür gedacht, auf Dauer Ihre lokale Exchange-Umgebung parallel zu Exchange Online zu betreiben. Es geht dabei also in erster Linie nicht darum, alle Postfächer zu Exchange Online zu migrieren. So könnten Sie Ihre Postfächer auf beide Umgebungen verteilen, Archive für lokale Postfächer in Exchange Online anlegen etc. In einer Hybridkonfiguration können Sie die Postfächer jederzeit zwischen den beiden Umgebungen verschieben – so wäre auch eine Migration denkbar, und die Outlook-Profile müssten nicht neu erstellt werden. Damit die Anwender dabei nicht eingeschränkt werden, je nachdem wo ihr Postfach liegt (beispielsweise möchte ein Anwender, der sein Postfach in Exchange Online hat, durchaus gerne die freien Zeiten im Kalender eines Postfachs auf dem lokalen Exchange Server einsehen), ist eine recht komplexe Konfiguration der beiden Exchange-Umgebungen erforderlich – für die reine Migration gestaltete sich dies recht aufwendig.

Neben diesen historisch schon länger verfügbaren Migrationsmethoden gibt es zusätzlich noch die *Minimale Hybridkonfiguration* und die *Express-Hybridkonfiguration*, die hinsichtlich der Konfiguration stark vereinfachte Varianten der an sich komplexen Hybridkonfiguration sind. Sie sind weniger aufwendig, da nicht alle Funktionen einer auf Dauer angelegten Hybridkonfiguration konfiguriert werden, haben aber gegenüber den alten Methoden große Vorteile:

- ▶ Die Outlook-Profilen müssen nicht neu erstellt werden.
- ▶ Unterstützt wird Exchange ab 2010.
- ▶ Die Minimale Hybridkonfiguration kann wie die mehrstufige Migration auch für größere Umgebungen eingesetzt werden.

Sehen wir uns die Migrationsmethoden nun etwas genauer an.

6.9.1 Verfahrensübersicht

Exchange Online bietet Ihnen vier verschiedene Exchange-Migrationsverfahren an, die alle das Ziel haben, sämtliche relevanten lokalen Postfächer zu Exchange Online zu übertragen. Tabelle 6.17 zeigt die wichtigsten Unterschiede auf. Sie liefert einen Anhaltspunkt dafür, welche der Verfahren für Ihre Umgebung möglicherweise in Betracht kommen.

| Merkmal | Übernahme-migration (altes Verfahren) | Mehrstufige Migration (altes Verfahren) | Express-Hybrid-konfiguration (neues Verfahren) | Minimale Hybrid-konfiguration (neues Verfahren) |
|--------------------------------------|--|--|---|--|
| Von Exchange 2003 | Ja | Ja | Nein | Nein |
| Von Exchange 2007 | Ja | Ja | Nein | Nein |
| Von Exchange 2010 | Ja | Nein | Ja | Ja |
| Von Exchange 2013 | Ja | Nein | Ja | Ja |
| Von Exchange 2016 | Ja | Nein | Ja | Ja |
| Von Exchange 2019 | Ja | Nein | Ja | Ja |
| Empfohlene Anzahl Postfächer | bis 150 | 150 bis 5.000 | bis 150 | 150 bis 5.000 |
| Maximale Anzahl Postfächer pro Batch | 2.000 | 2.000 | – | – |

Tabelle 6.17 Unterschiede zwischen den Migrationsverfahren

| Merkmal | Übernahme-migration (altes Verfahren) | Mehrstufige Migration (altes Verfahren) | Express-Hybrid-konfiguration (neues Verfahren) | Minimale Hybrid-konfiguration (neues Verfahren) |
|---|--|--|---|--|
| Auswahl der zu migrierenden Postfächer | Nein | Ja | Ja | Ja |
| Typischer Migrationszeitraum | wenige Tage | einige Wochen | wenige Tage | einige Wochen |
| Migrationsverwaltung über das EAC | Ja | Ja | Nein | Nein |
| Migrationsverwaltung über das Microsoft 365 Admin Center | Nein | Nein | Ja | Ja |
| Active Directory-Synchronisierung erforderlich | Nein | Ja | Ja (einmalig zur Migration) | Ja |
| Mailaustausch zwischen beiden Exchange-Umgebungen | Nein | Ja | Ja | Ja |
| Kombinierte globale Adressliste | Nein | Ja | Ja | Ja |
| Übergreifender Zugriff auf Frei-/Gebucht-Informationen | Nein | Nein | Nein | Nein |
| Automatische Umleitung von Outlook im Web und Active-Sync | Nein | Nein | Nein | Nein |

Tabelle 6.17 Unterschiede zwischen den Migrationsverfahren (Forts.)

| Merkmals | Übernahme-migration (altes Verfahren) | Mehrstufige Migration (altes Verfahren) | Express-Hybrid-konfiguration (neues Verfahren) | Minimale Hybrid-konfiguration (neues Verfahren) |
|---|--|--|---|--|
| Weiterverwendung von Outlook-OST-Dateien (lokaler Cache von Exchange-Postfächern) | Nein | Nein | Ja | Ja |
| Übergreifende Suche in Postfächern (eDiscovery) | Nein | Nein | Nein | Nein |
| TLS-(Transport Layer Security-)verschlüsselter E-Mail-Verkehr | Nein | Nein | Nein | Nein |

Tabelle 6.17 Unterschiede zwischen den Migrationsverfahren (Forts.)

In der Tabelle sind einige Punkte besonders bemerkenswert:

► **Auswahl der zu migrierenden Postfächer**

Bei der Übernahmемigration können Sie keine bestimmten Postfächer für die Migration auswählen. Stattdessen werden mit Ausnahme der Systempostfächer alle Postfächer migriert.

► **Outlook-OST-Dateien**

Outlook legt auf dem lokalen Computer eine OST-Datei an, die als Cache fungiert, wenn eine Verbindung zum Exchange Server nicht möglich ist. Somit kann der Anwender mit seinem Postfach auch offline arbeiten. Bei der Übernahmемigration und der mehrstufigen Migration kann eine bestehende OST-Datei nach der Exchange Online-Migration weiterverwendet werden. Für Exchange Online wird in Outlook ein neues Profil angelegt und damit auch eine neue OST-Datei. Beachten Sie diesen Umstand bei der Berücksichtigung der zu erwartenden Up- und Downloadkapazität, denn diese wird dadurch oftmals verdoppelt: Die Daten der Postfächer der lokalen Exchange-Umgebung müssen zuerst nach Exchange Online hochgeladen und dann von da wieder zu Outlook heruntergeladen werden.



Erfahrungswerte zur zu erwartenden Migrationsgeschwindigkeit finden Sie unter folgender URL:

<https://docs.microsoft.com/de-de/Exchange/mailbox-migration/office-365-migration-best-practices>

In den folgenden Abschnitten beschreibe ich die Durchführung der Migrationsverfahren.

6.9.2 Übernahmемigration

Bei der Übernahmемigration (engl. *Cutover Migration*) werden alle Postfächer (mit Ausnahme der Systempostfächer) von der lokalen Exchange-Umgebung in einem Schritt zu Exchange Online transferiert. Eine Auswahl der Postfächer ist nicht möglich.

Beachten Sie bitte, dass die Übernahmемigration nur möglich ist, wenn die Active Directory-Synchronisierung nicht aktiviert wurde.

Vor der Übernahmемigration müssen Sie die folgenden Voraussetzungen schaffen:

1. **die DNS-TTL für den MX-Eintrag herabsetzen**

Sind die Inhalte der Exchange-Postfächer übertragen, müssen Sie den MX-Eintrag Ihrer Domäne, der zunächst noch auf Ihren Exchange Server zeigt, umändern auf Exchange Online. Damit diese Änderung möglichst schnell in der DNS-Infrastruktur bekannt wird, sollten Sie den TTL-Wert des Eintrags herabsetzen, beispielsweise auf eine Stunde. Allerdings ist das nicht in jeder DNS-Verwaltung möglich.

2. **Outlook Anywhere aktivieren**

Falls noch nicht ausgeführt, müssen Sie auf der Quell-Exchange-Umgebung Outlook Anywhere aktivieren. Wie das beispielsweise bei Exchange 2010 geht, können Sie unter folgender URL nachlesen: [https://docs.microsoft.com/de-de/previous-versions/office/exchange-server-2010/bb123542\(v=exchg.141\)](https://docs.microsoft.com/de-de/previous-versions/office/exchange-server-2010/bb123542(v=exchg.141))

Ab Exchange 2013 ist Outlook Anywhere standardmäßig immer aktiv.

Für Outlook Anywhere ist bei der Exchange Online-Migration ein kommerzielles Zertifikat einer öffentlichen Zertifizierungsstelle erforderlich. Beachten Sie, dass es sich dabei nicht um ein selbst signiertes Zertifikat handeln darf.

3. **AutoErmittlung aktivieren**

Ab Exchange 2007 sollten Sie darüber hinaus die Funktion *AutoErmittlung* aktivieren (*Autodiscover*), um ein einfaches Auffinden der Quell-Exchange-Umgebung zu ermöglichen.

4. **Deaktivieren von Unified Messaging**

Bei den zu migrierenden Postfächern darf Unified Messaging nicht aktiviert sein.

5. **Migrationsbenutzer auswählen und berechtigen**

Bei der Migration müssen Sie einen lokalen Benutzer angeben, der auf alle Postfächer die Zugriffsrechte *Vollzugriff* oder *Empfangen als* hat. Falls erforderlich, berechtigen Sie den Benutzer, unter dem Sie die Migration durchführen wollen.

Verbindungseinstellungen überprüfen

Damit der Exchange Online-Migrations-Assistent auf die Postfächer einer lokalen Exchange-Umgebung zugreifen kann, müssen Outlook Anywhere und gegebenenfalls die AutoErmittlung richtig konfiguriert sein. Um das zu überprüfen, können Sie den *Microsoft Remote*

Connectivity Analyzer (RCA) zurückerufen. Dabei handelt es sich um eine Webanwendung, die Sie unter folgender URL erreichen (siehe Abbildung 6.90):

<https://testconnectivity.microsoft.com>

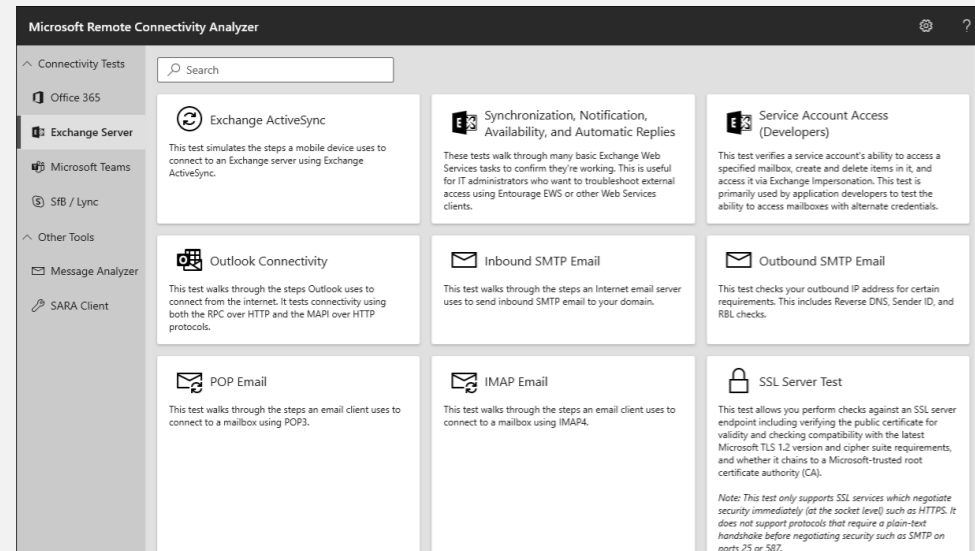


Abbildung 6.90 Remote Connectivity Analyzer

Mithilfe des RCA erhalten Sie bei typischen Verbindungsproblemen einen Hinweis auf die Ursache. Dazu bietet das Tool für lokale Exchange Server unterschiedliche Tests an:

- ▶ Exchange ActiveSync
- ▶ Synchronisierung, Benachrichtigung, Verfügbarkeit und automatische Antworten (Abwesenheitsnachrichten)
- ▶ Dienstkontozugriff (Entwickler)
- ▶ Outlook-Verbindung
- ▶ eingehende SMTP-E-Mail
- ▶ ausgehende SMTP-E-Mail
- ▶ POP3
- ▶ IMAP
- ▶ SSL

Bei der Exchange-Migration ist beispielsweise der ActiveSync-Test sehr hilfreich, um Hinweise darauf zu erhalten, warum der Migrations-Assistent keine Verbindung zur lokalen Exchange-Umgebung aufbauen kann. Ein Beispiel für die Ausgabe sehen Sie in Abbildung 6.91.

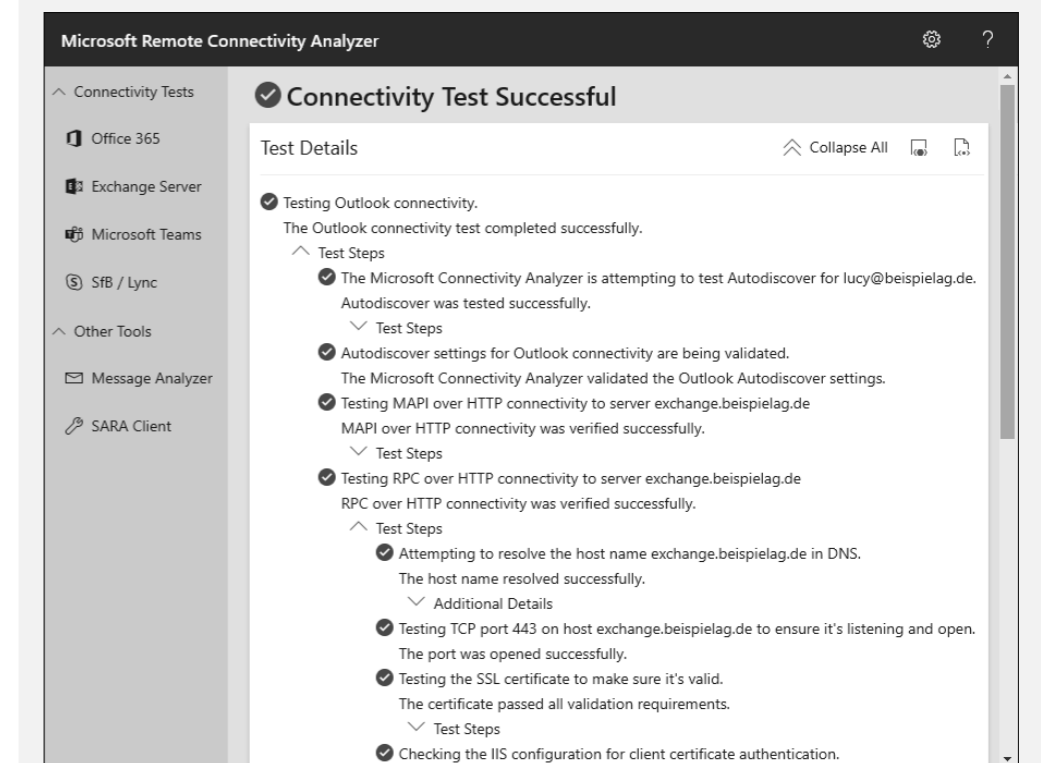


Abbildung 6.91 Testergebnis der Outlook-Verbindung

Bei der Migration werden folgende Elemente in das Zielpostfach übertragen:

- ▶ E-Mails und Ordner
- ▶ Regeln und Kategorien
- ▶ Kalendereinträge
- ▶ Abwesenheitsnachrichten
- ▶ Kontakte
- ▶ Aufgaben
- ▶ Delegationen und Ordnerberechtigungen
- ▶ Outlook-Einstellungen

Dagegen werden die folgenden Elemente nicht übertragen:

- ▶ Sicherheitsgruppen
- ▶ dynamische Verteilerlisten
- ▶ Systempostfächer

- ▶ Dumpster-Inhalte (siehe Abschnitt 6.8.3, »Gelöschte Elemente«)
- ▶ *Senden als*-Berechtigungen

Migrationsvorgang

Den Vorgang bei der Übernahmemigration stellt Abbildung 6.92 dar.

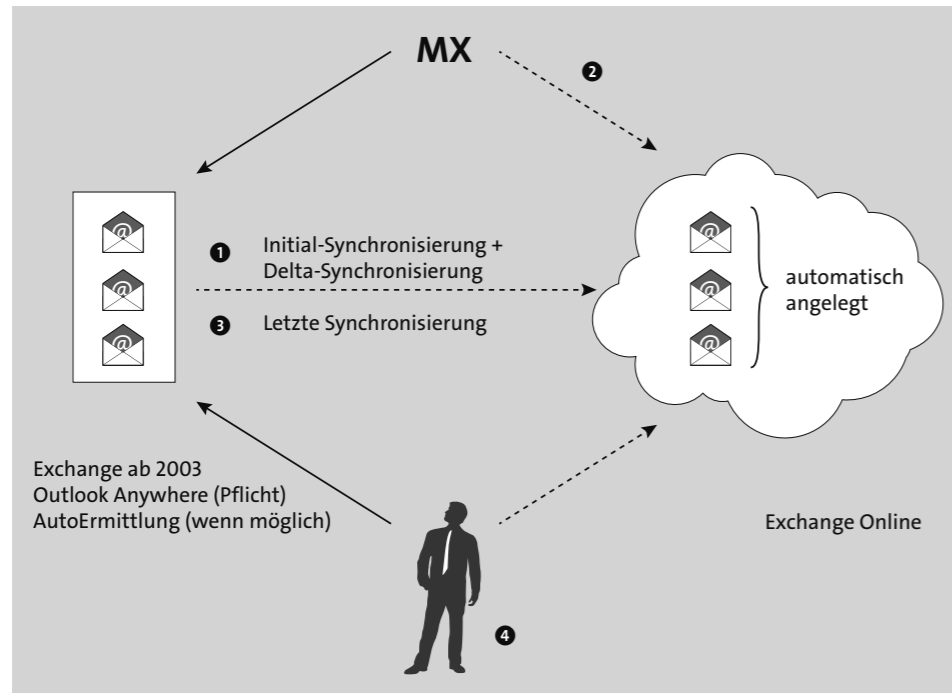


Abbildung 6.92 Die Übernahmemigration erfolgt in vier Schritten.

Die einzelnen Schritte haben folgende Bedeutung:

1 Datenmigration

Mithilfe des Exchange Online-Migrations-Assistenten oder der PowerShell werden die Verbindungsdaten zur Quell-Exchange-Umgebung angegeben. Der Migrations-Assistent wird dann entsprechende Postfächer in Exchange Online anlegen. Danach wird wie bei der IMAP-Migration zunächst der aktuelle Inhalt der Postfächer übertragen (*Initial-Synchronisierung*) – diesmal nicht nur E-Mails, sondern alle Elemente. Eine Filterung auf bestimmte Ordner ist jedoch nicht möglich. Im Anschluss erfolgt einmal am Tag eine *Delta-Synchronisierung*, um die bis dahin aufgelaufenen Änderungen abzugleichen.

2 Ändern der DNS-Einträge

Der MX-Eintrag sowie die AutoErmittlungs-Einträge der E-Mail-Domäne werden geändert, sodass sie auf Exchange Online zeigen und nicht mehr auf die Quell-Exchange-Umgebung.

3 Abschließen der Migration

Sie schließen die Migration ab und synchronisieren dabei die letzten Änderungen.

4 Benutzerlizenzierung

Bei der Übernahmemigration legt der Migrations-Assistent selbstständig Postfächer samt Microsoft 365-Benutzer an. Diese werden jedoch nicht lizenziert, was Sie selbst über das Microsoft 365 Admin Center bzw. Microsoft 365-Portal oder die PowerShell vornehmen müssen.

Sehen wir uns nun die erforderlichen Schritte genauer an.

Schritt 1: Datenmigration

Die Datenmigration können Sie wie bei der IMAP-Migration wahlweise im EAC oder mit der PowerShell durchführen. Beginnen wir wieder mit dem Ansatz über das EAC. Im Anschluss zeige ich Ihnen die PowerShell-Alternative.

1. Öffnen Sie im EAC den Bereich MIGRATION (siehe Abbildung 6.93).

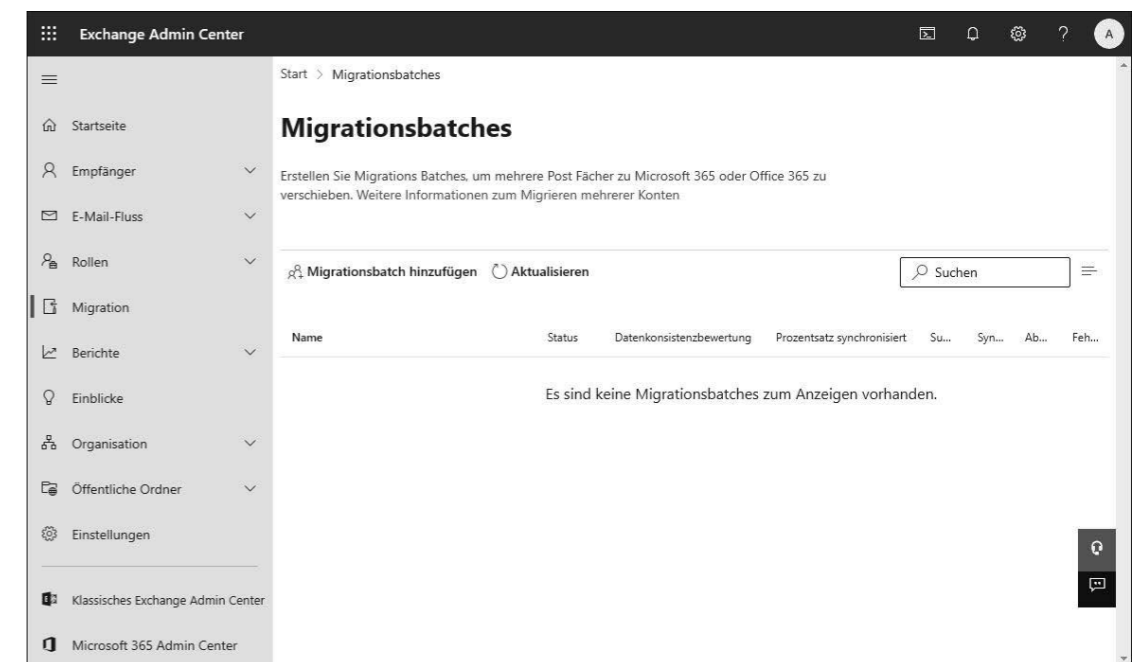


Abbildung 6.93 E-Mail-Migration im Exchange Admin Center (EAC)

2. Klicken Sie auf MIGRATIONSbatch HINZUFÜGEN, erscheint der E-Mail-Migrations-Assistent (siehe Abbildung 6.94).

Im Schritt MIGRATIONSPfad geben Sie dem Migrationsbatch einen Namen und wählen beim POSTFACH-MIGRATIONSPfad die Option MIGRATION ZU EXCHANGE ONLINE.

Abbildung 6.94 E-Mail-Migrations-Assistent

3. Im Schritt **MIGRATIONSTYP** wählen Sie den Typ **CUTOVER-MIGRATION** (siehe Abbildung 6.95).

Abbildung 6.95 Migrationstyp

4. Im Schritt **VORAUSSETZUNGEN** informieren Sie sich über eben diese (siehe Abbildung 6.96).

Abbildung 6.96 Voraussetzungen

5. Im Schritt **MIGRATIONSENDPUNKT** wählen Sie die Option zum **ERSTELLEN EINES NEUEN MIGRATIONSENDPUNKTS** (siehe Abbildung 6.97).

Abbildung 6.97 Migrationsendpunkt

Geben Sie die E-Mail-Adresse eines zu migrierenden Benutzers an (mithilfe der Adresse werden über die AutoErmittlung die Servereinstellungen abgefragt) sowie den Benutzernamen und das Kennwort des Migrationsbenutzers auf dem Quell-Exchange-Server.

- Der Assistent zeigt die über die AutoErmittlung erkannten Servereinstellungen an (siehe Abbildung 6.98). Sollten Sie die AutoErmittlung auf dem Quell-Exchange-Server nicht aktiviert haben, müssen Sie die Einstellungen selbst angeben.

Abbildung 6.98 Migrationsendpunkt bestätigen

Sollte der Migrations-Assistent Probleme bei der Verbindung feststellen, erhalten Sie eine Fehlermeldung – allerdings im Regelfall eine nichtssagende. Hier ist es oftmals hilfreich, auf die PowerShell auszuweichen. Dort gibt es das Cmdlet `Test-MigrationServerAvailability`, das ebenfalls die Verbindungseinstellungen überprüft, aber deutlich aussagekräftigere Fehlermeldungen liefert. Wie das Cmdlet eingesetzt wird, erfahren Sie im Folgenden, wenn es um die Übernahm migration mit der PowerShell geht.

- Im Schritt **BENUTZER HINZUFÜGEN** laden Sie eine CSV-Datei mit den zu migrierenden Benutzerkonten hoch (Abbildung 6.99). Erstellen Sie dazu in der CSV-Datei eine einzelne Spalte mit der Überschrift `EmailAddress` und in den Zeilen die E-Mail-Adresse der zu importierenden Benutzer.

Abbildung 6.99 Benutzer hinzufügen

- Im Schritt **KONFIGURATION** geben Sie die **ZIELZUSTELLUNGSDOMÄNE** an (siehe Abbildung 6.100). Achtung: Geben Sie hier nicht (!) Ihre eigene Domäne an, sondern die Domäne mit der Endung `mail.onmicrosoft.com`.
- Im letzten Schritt, **PLANEN**, können Sie noch einen Microsoft 365-Benutzer auswählen, der über den Fortschritt der Migration per E-Mail benachrichtigt wird. Dieses Angebot sollten Sie wahrnehmen, um bei Fehlern und bei der Fertigstellung frühzeitig informiert zu werden. Außerdem entscheiden Sie, ob die Migration unmittelbar oder zu einem späteren Zeitpunkt begonnen werden soll (siehe Abbildung 6.101).
- Falls Sie sich für einen späteren Start der Migration entschieden haben, markieren Sie den Migrationsbatch und starten ihn, um mit der Migration zu beginnen.

Je nach Anzahl und Kapazität der Quellpostfächer sowie der zur Verfügung stehenden Internetbandbreite dauert die Migration nun entsprechend lange.

Als Nächstes folgt die Änderung der DNS-Einträge.

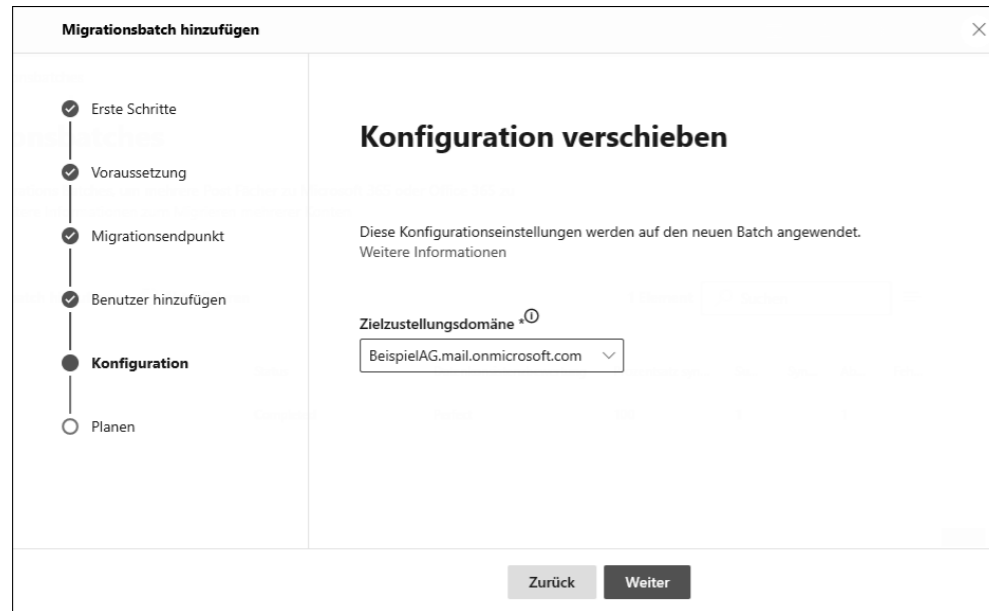


Abbildung 6.100 Konfiguration

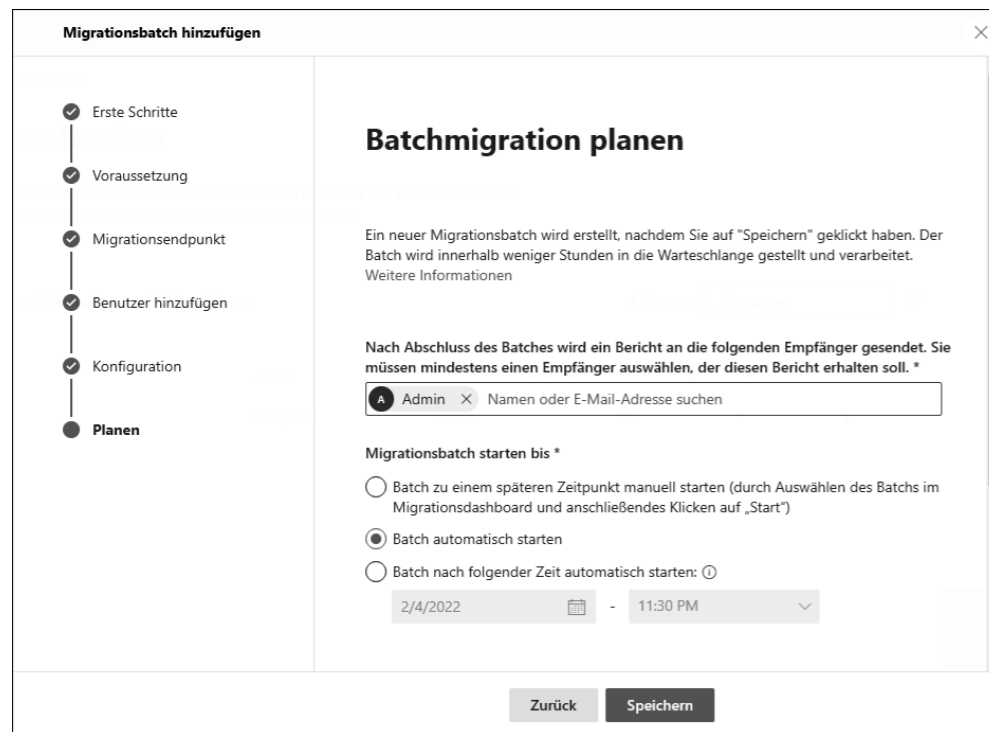


Abbildung 6.101 Planen

Schritt 2: Ändern der DNS-Einträge

Ändern Sie den MX-Eintrag sowie die AutoErmittlungs-Einträge in den Einstellungen Ihres DNS-Anbieters entsprechend den Vorgaben von Microsoft 365.

Vergessen Sie dabei nicht Ihren internen DNS-Server, sofern dort auch ein AutoErmittlungs-Eintrag vorhanden ist. Ansonsten bekommen die internen Clients Probleme bei der Verbindung mit Exchange Online, da sie sich nach wie vor bei der alten Umgebung anmelden.

Danach sollten Sie warten, bis sich die Änderung in der DNS-Infrastruktur verbreitet hat. Dies kann bis zu drei Tage dauern. Anschließend können Sie die Migration abschließen. Wie die DNS-Einträge aussehen sollen, können Sie in Abschnitt 2.4, »Domänenverwaltung«, nachlesen.

Schritt 3: Abschließen der Migration

Nachdem Sie sichergestellt haben, dass neue E-Mails in den Exchange Online-Postfächern ankommen, können Sie die Migration abschließen.

1. Öffnen Sie im EAC den Bereich MIGRATION.
2. Warten Sie eine letzte Synchronisierung ab, nachdem die Änderung am MX-DNS-Eintrag aktiv wurde (und das kann bis zu drei Tage dauern). Beenden Sie dann den Migrationsbatch.
3. Zu guter Letzt sollten Sie auf Ihrer internen Exchange-Umgebung die URI für die Auto-Ermittlung mit folgendem PowerShell-Kommando zurücksetzen:

```
Set-ClientAccessServer -AutodiscoverInternalConnectionURI $Null
```

Listing 6.49 Zurücksetzen der AutoErmittlungs-URI

Damit ist es geschafft – die Übernahm migration ist abgeschlossen. Ihre Anwender müssen nun gegebenenfalls ihre E-Mail-Software für Exchange Online konfigurieren, sofern nicht nur Outlook im Web zum Einsatz kommen soll. Für Outlook bedeutet dies das Anlegen eines neuen Profils.

Schritt 4: Benutzerlizenzierung

Die automatisch mit dem Migrations-Assistenten angelegten Benutzer werden nicht lizenziert. Während einer Übergangsphase ist das kein Problem (siehe Abschnitt 6.5.1, »Postfächer«) – in dieser Zeit können die Anwender uneingeschränkt mit ihren neuen Postfächern arbeiten. So haben Sie genügend Zeit, die Benutzerlizenzierung bei Gelegenheit vorzunehmen – nur vergessen sollten Sie sie nicht, sonst können Ihre Anwender eines Tages ihre Postfächer nicht mehr öffnen.

Zur Benutzerlizenzierung haben Sie zwei Möglichkeiten:

- ▶ Microsoft 365 Admin Center (siehe Abschnitt 2.5.2, »Benutzer anlegen«)
- ▶ PowerShell (siehe Abschnitt 3.14.4, »Benutzer anlegen«)

Übernahmemigration mit der PowerShell

Die Übernahmemigration ist auch mit der PowerShell durchführbar. Hier sehen Sie zunächst ein Beispiel für den Programmcode:

```
$mail = "lucy@beispielag.de"

#Verbindung testen
$cred = Get-Credential
Test-MigrationServerAvailability -Autodiscover `
  -EmailAddress $mail `
  -Credentials $cred `
  -ExchangeOutlookAnywhere

#Endpunkt anlegen
$endpunkt = New-MigrationEndpoint -ExchangeOutlookAnywhere `
  -Name "Endpunkt" `
  -Autodiscover `
  -EmailAddress $mail `
  -Credentials $cred

#Batch anlegen
$batch = New-MigrationBatch -Name "Batch" `
  -SourceEndpoint $endpunkt.Identity

#Batch starten
Start-MigrationBatch -Identity $batch.Identity.Id

#Batch-Status abfragen
Get-MigrationBatch -Identity $batch.Identity.Id

#Batch beenden (Achtung: Erst zum gegebenen Zeitpunkt!)
Stop-MigrationBatch -Identity $batch.Identity.Id

#Batch löschen (Achtung: Erst zum gegebenen Zeitpunkt!)
Remove-MigrationBatch -Identity $batch.Identity.Id
```

Listing 6.50 Übernahmemigration

Hierzu möchte ich noch einiges erklären:

- Das Cmdlet `Test-MigrationServerAvailability` überprüft die Verbindungseinstellungen zur Quell-Exchange-Umgebung. In diesem Beispiel wird die AutoErmittlung verwendet.

Ist die AutoErmittlung nicht aktiviert, können Sie über andere Parameter die Verbindungseinstellungen manuell angeben. Beim Parameter `-EmailAddress` geben Sie eine E-Mail-Adresse für die AutoErmittlung an und unter `-Credentials` die Anmeldedaten eines Benutzerkontos, das auf alle Postfächer der Quell-Exchange-Umgebung Zugriff hat.

- Für den Zugriff auf Exchange wird mit `New-MigrationEndpoint` ein neuer Migrationsendpunkt angelegt. Mit dem Parameter `-Name` geben Sie dem Endpunkt einen Namen, unter dem Sie ihn im EAC auch wiederfinden.
- Mit dem Cmdlet `New-MigrationBatch` legen Sie weitere Migrationsoptionen fest. Lassen Sie sich vom Begriff *Batch* nicht verwirren. Die Übernahmemigration wird nicht in Abschnitten (Batches) durchgeführt, sondern in einem Rutsch. Mit dem Parameter `-Name` geben Sie eine Bezeichnung für den Migrationsvorgang an.
- Mit dem Cmdlet `Start-MigrationBatch` starten Sie die eigentliche Migration. Mit `Get-MigrationBatch` fragen Sie den Status ab, `Stop-MigrationBatch` beendet den Batch, und `Remove-MigrationBatch` entfernt ihn.

6.9.3 Mehrstufige Migration

Als Variante zur Übernahmemigration steht Ihnen die mehrstufige Migration zur Verfügung (engl. *Staged Migration*). Bitte beachten Sie, dass diese nur zum Einsatz kommen kann, wenn die Active Directory-Synchronisierung aktiviert wurde (siehe Abschnitt 4.2.1, »Verzeichnis-synchronisierung«).

Dieses Verfahren eignet sich nicht, wenn Sie mit einem Exchange Server in den Versionen ab 2010 arbeiten. Der Grund dafür liegt beim Protokoll *NSPI (Named Service Provider Interface)*, das bei diesen Versionen nur schreibgeschützte Operationen zulässt. Die mehrstufige Migration erfordert aber schreibende Operationen.

Bei der mehrstufigen Migration müssen nicht alle Postfächer in einem Rutsch zu Exchange Online migriert werden, sondern in mehreren Blöcken (Migrationsbatches). In manchen Szenarien ist das erforderlich, beispielsweise wenn die zu migrierende Kapazität der Quellpostfächer zu groß ist, um sie an einem Wochenende zu migrieren. Sie können die Migration z. B. auch abteilungsweise vornehmen und die Mitarbeiter jeweils für Microsoft 365 schulen, nachdem oder kurz bevor sie migriert wurden.

Welche Postfächer jeweils zu einem Migrationsbatch gehören, legen Sie in CSV-Dateien fest.

Die Voraussetzungen für die mehrstufige Migration ähneln denen für die Übernahmemigration:

1. die DNS-TTL für den MX-Eintrag herabsetzen
2. Outlook Anywhere aktivieren
3. AutoErmittlung aktivieren

4. Unified Messaging deaktivieren
5. Migrationsbenutzer auswählen und berechtigen
6. die Active-Directory-Synchronisierung aktivieren
7. CSV-Dateien für Migrationsbatches anlegen

Die Schritte 1 bis 6 können Sie in Abschnitt 6.9.2, »Übernahm migration«, nachlesen. Auch welche Elemente und Einstellungen migriert werden und welche nicht, ist dort beschrieben. Den erforderlichen Aufbau der CSV-Dateien in Schritt 7 finden Sie im folgenden Abschnitt.

Der Aufbau der CSV-Dateien

Für die jeweiligen Blöcke aus zu migrierenden Postfächern benötigen Sie jeweils eine CSV-Datei. Der Aufbau dieser Blöcke muss wie folgt aussehen:

```
EmailAddress,Password,ForceChangePassword
```

Listing 6.51 Die CSV-Datei enthält drei Felder.

Tabelle 6.18 erläutert die Bedeutung der einzelnen Felder.

| Feld | Bedeutung |
|---------------------|---|
| EmailAddress | Die E-Mail-Adresse des Quellpostfachs in der bisherigen Exchange-Umgebung |
| Password | Das Kennwort des Microsoft 365-Benutzerkontos wird auf diesen Wert gesetzt (optional). Sollten Sie einen Domänenverbund für Single Sign-on eingerichtet haben, vergeben Sie hier kein Kennwort. |
| ForceChangePassword | Angabe, ob das Kennwort des Exchange Online-Postfachs bei der ersten Anmeldung geändert werden muss (True) oder nicht (False) (optional). Haben Sie einen Domänenverbund für Single Sign-on eingerichtet, muss der Wert False sein. |

Tabelle 6.18 Aufbau der CSV-Datei

Pro CSV-Datei dürfen Sie maximal 1.000 Postfächer angeben.

Der Migrationsvorgang

Nachdem Sie alle Vorbereitungen getroffen haben, können Sie die Migration durchführen. Diese lässt sich in fünf Schritte unterteilen, die Sie auch in Abbildung 6.102 sehen.

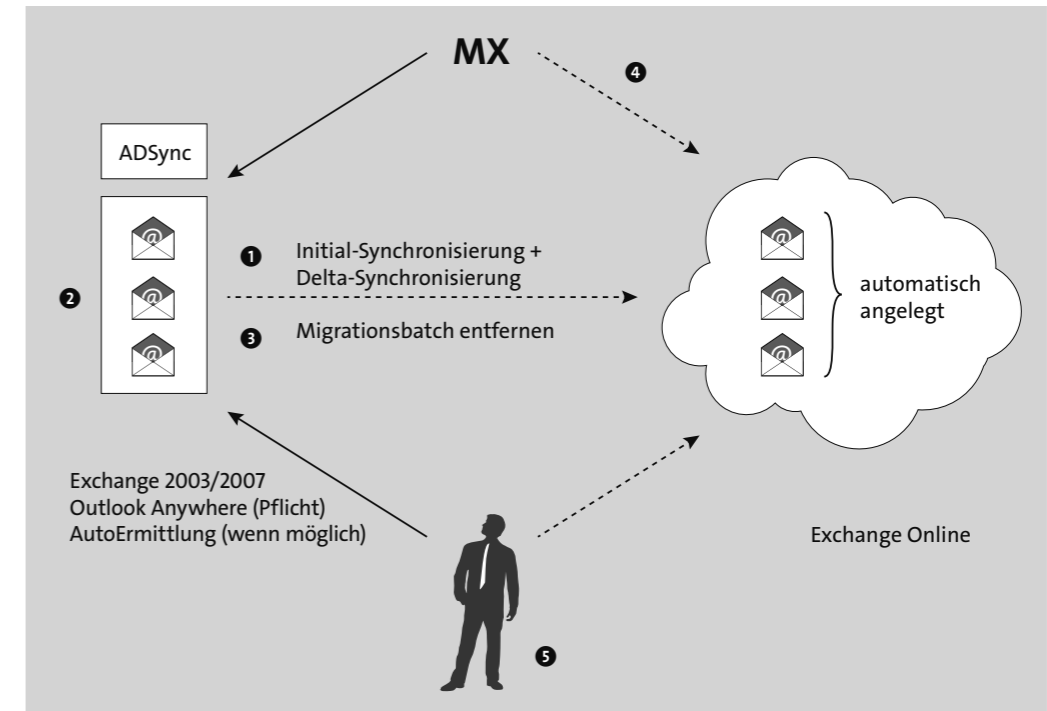


Abbildung 6.102 Ablaufschema für die mehrstufige Migration

1 Datenmigration

Anhand der Angaben einer oder mehrerer CSV-Dateien werden die E-Mails aus vorhandenen Exchange-Postfächern in die Exchange Online-Postfächer migriert.

Bei den alten Exchange-Postfächern wird die Eigenschaft `TargetAddress` automatisch so gesetzt, dass in der alten Exchange-Umgebung eintreffende Mails automatisch zu Exchange Online weitergeleitet werden. Die Anwender können sofort mit ihren neuen Exchange Online-Postfächern arbeiten.

2 Konvertieren der Postfächer in E-Mail-aktivierte Benutzer

Nach der Übertragung der Daten aus den alten Postfächern sollten Sie die Postfächer in E-Mail-aktivierte Benutzer umwandeln, damit Ihre Anwender nicht weiter mit den alten Postfächern arbeiten. Die AutoErmittlung würde aber nach wie vor zur alten Exchange-Umgebung weiterleiten.

Die Datenmigration erfolgt in Batches, die Sie mithilfe der CSV-Dateien angeben.

3 Löschen der abgeschlossenen Migrationsbatches

Vollständig abgearbeitete Migrationsbatches können nun entfernt werden.

4 Ändern der DNS-Einträge

Nachdem alle Migrationsbatches verarbeitet wurden, folgt die Änderung des MX-Eintrags sowie des AutoErmittlungs-Eintrags. Durch diese Änderung in den DNS-Einstellungen Ihres DNS-Anbieters sorgen Sie dafür, dass neue E-Mails nicht mehr bei der alten Exchange-Umgebung ausgeliefert werden, sondern in Exchange Online.

5 Benutzerlizenzierung

Falls es noch nicht geschehen ist, müssen Sie Ihre Microsoft 365-Benutzer mit einer passenden Exchange Online-Lizenz ausstatten.

Sehen wir uns die Schritte nun im Einzelnen an.

Schritt 1: Datenmigration

Die Datenmigration führen Sie wie bei der IMAP- und der Übernahmemigration entweder über den Migrations-Assistenten aus dem EAC durch oder über die PowerShell. Beginnen wir wieder mit dem EAC-Ansatz.

1. Öffnen Sie im EAC den Bereich MIGRATION (siehe Abbildung 6.103).

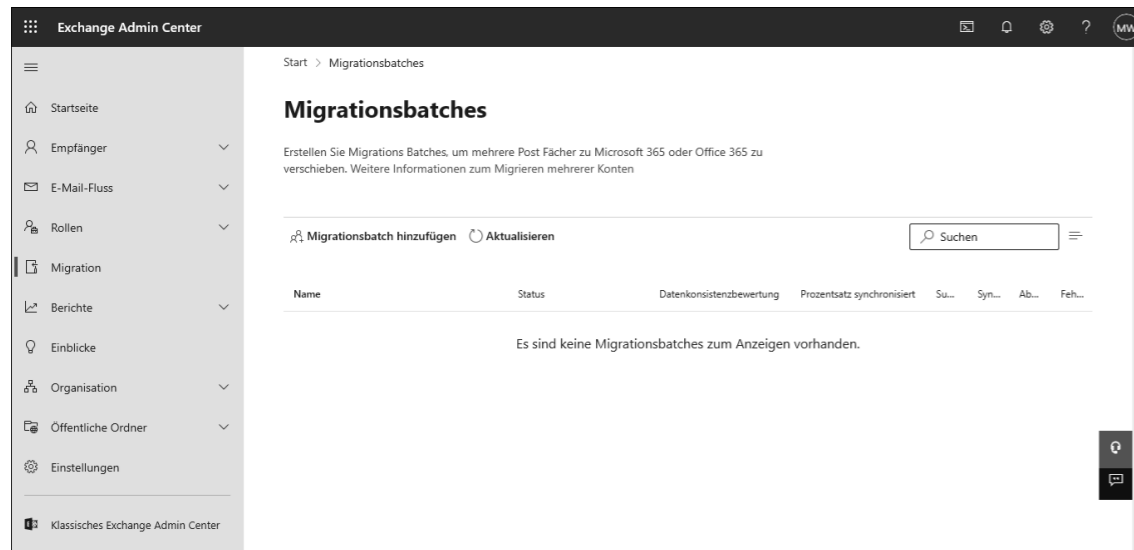


Abbildung 6.103 E-Mail-Migration im EAC

2. Wenn Sie auf MIGRATIONS BATCH HINZUFÜGEN klicken, erscheint der E-Mail-Migrations-Assistent (siehe Abbildung 6.104).

Im Schritt MIGRATIONSPFAD geben Sie dem Migrationsbatch einen Namen und wählen beim POSTFACH-MIGRATIONSPFAD die Option MIGRATION ZU EXCHANGE ONLINE.

3. Im Schritt MIGRATIONSTYP wählen Sie den Typ MEHRSTUFIGE MIGRATION (siehe Abbildung 6.105).

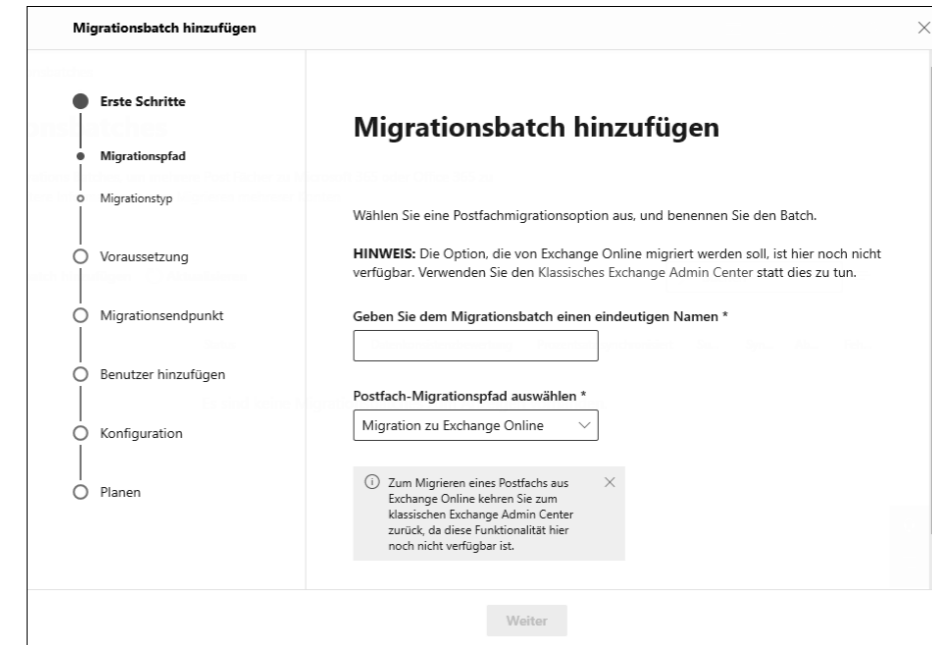


Abbildung 6.104 Der E-Mail-Migrations-Assistent

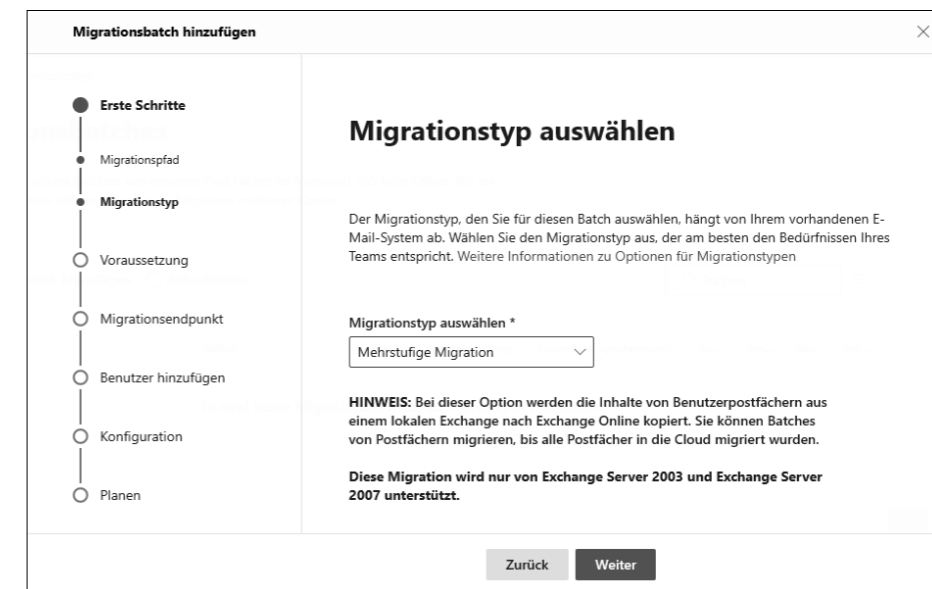


Abbildung 6.105 Migrationstyp

4. Im Schritt VORAUSSETZUNGEN informieren Sie sich über eben diese (siehe Abbildung 6.106).

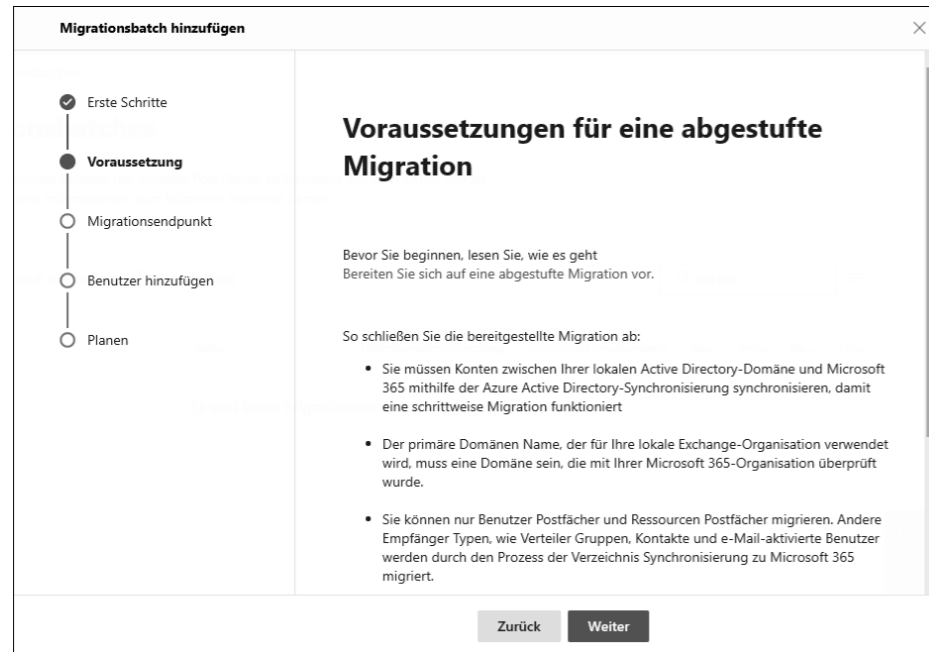


Abbildung 6.106 Voraussetzungen

5. Im Schritt MIGRATIONSENDPUNKT wählen Sie die Option zum ERSTELLEN EINES NEUEN MIGRATIONSENDPUNKTS (siehe Abbildung 6.107).

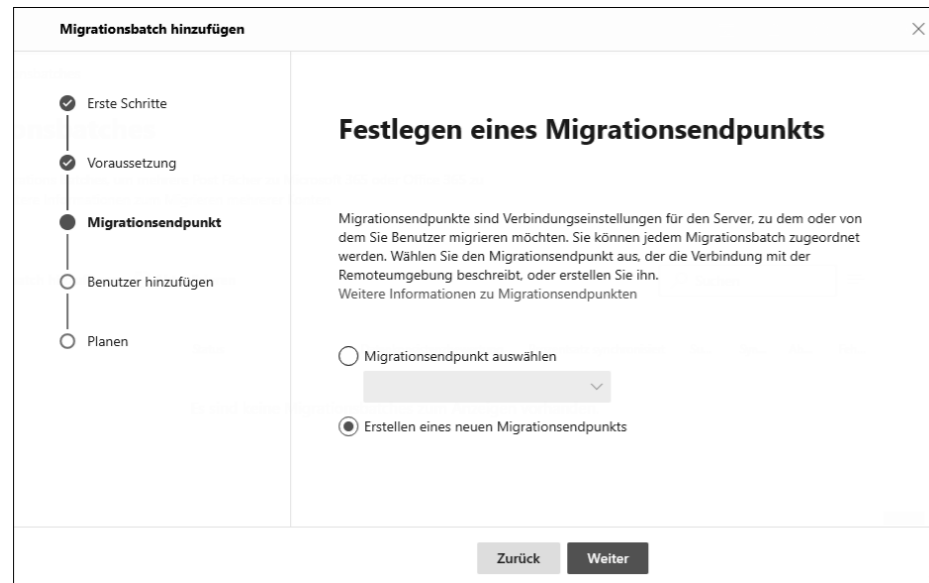


Abbildung 6.107 Migrationsendpunkt

Geben Sie die E-Mail-Adresse eines zu migrierenden Benutzers an (mithilfe der Adresse werden über die AutoErmittlung die Servereinstellungen abgefragt) sowie den Benutzer-namen und das Kennwort des Migrationsbenutzers auf dem Quell-Exchange-Server.

6. Der Assistent zeigt die über die AutoErmittlung erkannten Servereinstellungen an (siehe Abbildung 6.108). Sollten Sie die AutoErmittlung auf dem Quell-Exchange-Server nicht aktiviert haben, müssen Sie die Einstellungen selbst angeben.

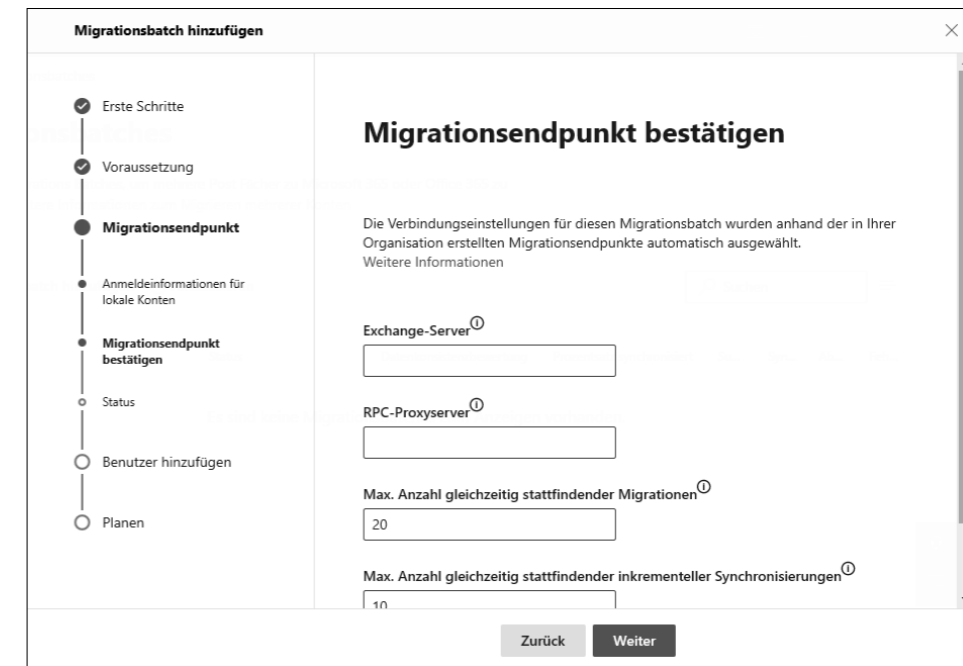


Abbildung 6.108 Migrationsendpunkt bestätigen

Sollte der Migrations-Assistent Probleme bei der Verbindung feststellen, erhalten Sie eine Fehlermeldung. Diese ist allerdings im Regelfall nichtssagend. Hier ist es oftmals hilfreich, auf die PowerShell auszuweichen. Dort gibt es das Cmdlet `Test-MigrationServerAvailability`, das ebenfalls die Verbindungseinstellungen überprüft, aber deutlich aussagekräftigere Fehlermeldungen liefert. Wie das Cmdlet eingesetzt wird, erfahren Sie im Folgenden, wenn es um die Übernahm migration mit der PowerShell geht.

7. Im Schritt BENUTZER HINZUFÜGEN laden Sie eine CSV-Datei mit den zu migrierenden Benutzerkonten hoch (Abbildung 6.109).
8. Im letzten Schritt, PLANEN, können Sie noch einen Microsoft 365-Benutzer auswählen, der über den Fortschritt der Migration per E-Mail benachrichtigt wird. Dieses Angebot sollten Sie wahrnehmen, um bei Fehlern und bei der Fertigstellung frühzeitig informiert zu werden. Außerdem entscheiden Sie, ob die Migration unmittelbar oder zu einem späteren Zeitpunkt begonnen werden soll (siehe Abbildung 6.110).

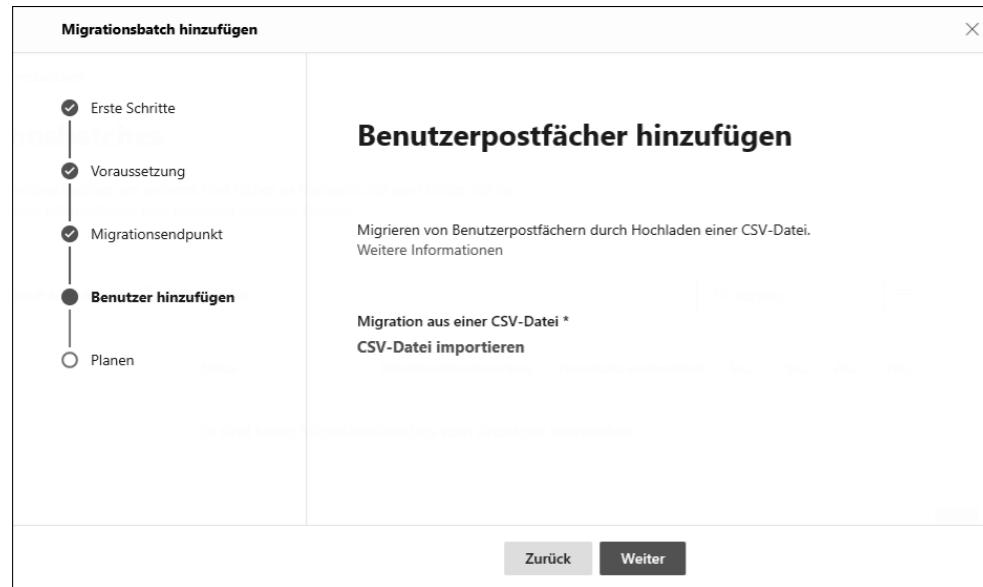


Abbildung 6.109 Benutzer hinzufügen

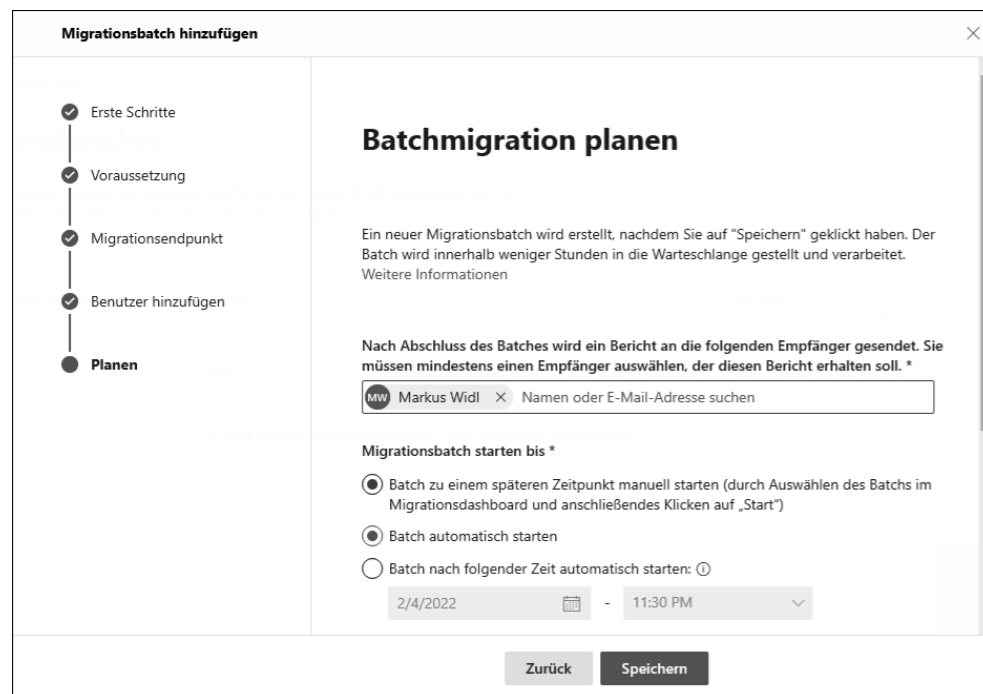


Abbildung 6.110 Planen

9. Falls Sie sich für einen späteren Start der Migration entschieden haben, markieren Sie den Migrationsbatch und starten ihn, um mit der Migration zu beginnen.

Je nach Anzahl und Kapazität der Quellpostfächer sowie der zur Verfügung stehenden Internetbandbreite dauert die Migration nun entsprechend lange.

Als Nächstes folgt das Konvertieren der Postfächer.

Schritt 2: Konvertieren der Postfächer in E-Mail-aktivierte Benutzer

Nachdem alle Postfächer aus der CSV-Datei migriert wurden, erhalten Sie eine Benachrichtigung an die zuvor angegebene E-Mail-Adresse. Jetzt sollten Sie die migrierten Postfächer in E-Mail-aktivierte Benutzer umwandeln, sodass Ihre Anwender nicht weiter mit den alten Postfächern arbeiten. Die AutoErmittlung würde aber nach wie vor zur alten Exchange-Umgebung weiterleiten. Mit der Umwandlung können auf den Clients neue Outlook-Profilen für Exchange Online angelegt werden.

1. Öffnen Sie im EAC im Bereich EMPFÄNGER den Abschnitt MIGRATION.
2. Markieren Sie den Migrationsbatch, und überprüfen Sie den Status. Steht dieser auf SYNCHRONISIERT, können Sie die Postfächer umwandeln.
3. Microsoft stellt PowerShell-Skripte bereit, um diesen Vorgang zu automatisieren. Die Skripte finden Sie unter folgenden URLs:

- für Exchange 2007: <https://docs.microsoft.com/de-de/Exchange/mailbox-migration/perform-a-staged-migration/convert-exchange-2007-mailboxes>
- für Exchange 2003: <https://docs.microsoft.com/de-de/Exchange/mailbox-migration/perform-a-staged-migration/convert-exchange-2003-mailboxes>

Sollten Sie beim Ausführen der Skriptdateien die Fehlermeldung erhalten, sie wären nicht digital signiert, öffnen Sie im Windows Explorer die Eigenschaften der Dateien und klicken auf der Registerkarte ALLGEMEIN auf die Schaltfläche ZULASSEN. Danach sollte die Fehlermeldung nicht mehr erscheinen. Wichtig ist, dass Sie diesen Vorgang für jede Datei einzeln und nicht gemeinsam durchführen.

Nach dem Umwandeln der alten Postfächer in E-Mail-aktivierte Benutzer können Sie mit einer weiteren CSV-Datei noch einmal den Vorgang starten.

Schritt 3: Löschen von abgeschlossenen Migrationsbatches

Nachdem Sie sichergestellt haben, dass neue E-Mails in den Exchange Online-Postfächern aufschlagen, können Sie die jeweiligen Migrationsbatches löschen.

1. Öffnen Sie im EAC im Bereich EMPFÄNGER den Abschnitt MIGRATION.
2. Markieren Sie den Migrationsbatch, und klicken Sie auf BEENDEN (Quadrat-Symbol). Ist der Status des Batches dann beendet, können Sie ihn LÖSCHEN (Mülltonnen-Symbol).

Schritt 4: Ändern der DNS-Einträge

Ändern Sie den MX-Eintrag sowie den AutoErmittlungs-Eintrag in den Einstellungen Ihres DNS-Anbieters entsprechend den Vorgaben von Microsoft 365.

Danach sollten Sie warten, bis sich die Änderung in der DNS-Infrastruktur verbreitet hat. Dies kann bis zu drei Tage dauern. Wie die DNS-Einträge aussehen sollen, können Sie in Abschnitt 2.4, »Domänenverwaltung«, nachlesen.



Vergessen Sie dabei nicht Ihren internen DNS-Server, sofern dort auch ein AutoErmittlungs-Eintrag vorhanden ist. Ansonsten bekommen die internen Clients Probleme bei der Verbindung mit Exchange Online, da sie sich nach wie vor bei der alten Umgebung anmelden.

Zu guter Letzt sollten Sie auf Ihrer internen Exchange-Umgebung die URI für die AutoErmittlung mit folgendem PowerShell-Kommando zurücksetzen:

```
Set-ClientAccessServer -AutodiscoverInternalConnectionURI $Null
```

Listing 6.52 Zurücksetzen der AutoErmittlungs-URI**Schritt 5: Benutzerlizenzierung**

Zur Benutzerlizenzierung haben Sie zwei Möglichkeiten:

- ▶ Microsoft 365 Admin Center (siehe Abschnitt 2.5.2, »Benutzer anlegen«)
- ▶ PowerShell (siehe Abschnitt 3.14.4, »Benutzer anlegen«)

Mehrstufige Migration mit der PowerShell

Die PowerShell-Variante bei der mehrstufigen Migration ähnelt einer Mischung aus der IMAP-Migration (wegen der CSV-Dateien) und der Übernahmemigration (wegen des anderen Verbindungsaufbaus). Listing 6.53 zeigt ein Beispiel:

```
$mail = "lucy@beispielag.de"
$datei = "Benutzer.csv"

#Verbindung testen
$cred = Get-Credential
Test-MigrationServerAvailability -Autodiscover `
  -EmailAddress $mail `
  -Credentials $cred `
  -ExchangeOutlookAnywhere

#Endpunkt anlegen
$endpunkt = New-MigrationEndpoint -ExchangeOutlookAnywhere `
  -Name "Endpunkt" `
  -Autodiscover `
  -EmailAddress $mail `
```

```
-Credentials $cred

#Batch anlegen
$batch = New-MigrationBatch -Name "Batch" `
  -SourceEndpoint $endpunkt.Identity `
  -CSVData ([System.IO.File]::ReadAllBytes($datei))

#Batch starten
Start-MigrationBatch -Identity $batch.Identity.Id

#Batch-Status abfragen
Get-MigrationBatch -Identity $batch.Identity.Id

#Batch beenden (Achtung: Erst zum gegebenen Zeitpunkt!)
Stop-MigrationBatch -Identity $batch.Identity.Id

#Batch löschen (Achtung: Erst zum gegebenen Zeitpunkt!)
Remove-MigrationBatch -Identity $batch.Identity.Id
```

Listing 6.53 Mehrstufige Migration

Zum Skript möchte ich noch einige Punkte erläutern:

- ▶ Das Cmdlet `Test-MigrationServerAvailability` überprüft die Verbindungseinstellungen zur Quell-Exchange-Umgebung. In diesem Beispiel wird die AutoErmittlung verwendet. Ist die AutoErmittlung nicht aktiviert, können Sie über andere Parameter die Verbindungseinstellungen manuell angeben. Beim Parameter `-EmailAddress` geben Sie eine E-Mail-Adresse für die AutoErmittlung an und unter `-Credentials` die Anmeldedaten eines Benutzerkontos, das auf alle Postfächer der Quell-Exchange-Umgebung Zugriff hat.
- ▶ Für den Zugriff auf Exchange wird mit `New-MigrationEndpoint` ein neuer Migrationsendpunkt angelegt. Mit dem Parameter `-Name` geben Sie dem Endpunkt einen Namen, unter dem Sie ihn im EAC auch wiederfinden.
- ▶ Mit dem Cmdlet `New-MigrationBatch` legen Sie weitere Migrationsoptionen fest. Mit dem Parameter `-Name` geben Sie eine Bezeichnung für den Migrationsvorgang an.
- ▶ Im Skript wird der Inhalt einer CSV-Datei eingelesen, aber nicht etwa über das Cmdlet `Import-CSV`, das Sie möglicherweise hier erwarten würden, sondern über einen Umweg: `[System.IO.File]::ReadAllBytes(...)`. Dabei greifen Sie auf die Klasse `System.IO.File` aus dem .NET Framework zu, genauer gesagt auf die statische Methode `ReadAllBytes` aus dieser Klasse. Dieser Umweg ist erforderlich, da das Cmdlet `New-MigrationBatch` die Daten als Byte-Array erwartet und nicht als die von `Import-CSV` gelieferten Objekte.

- ▶ Mit dem Cmdlet `Start-MigrationBatch` starten Sie die eigentliche Migration. Mit `Get-MigrationBatch` fragen Sie den Status ab, `Stop-MigrationBatch` beendet den Batch, und `Remove-MigrationBatch` entfernt ihn.

6.9.4 Minimale Hybridkonfiguration und Express-Hybridkonfiguration

In diesem Abschnitt beschreibe ich sowohl die Minimale Hybridkonfiguration als auch die Express-Hybridkonfiguration als Variante für kleine Unternehmen, die keine dauerhafte Verzeichnissynchronisierung benötigen.

Voraussetzungen

Die Voraussetzungen für die Migrationsmethoden sind die folgenden:

▶ Exchange-Version

Die lokale Exchange-Umgebung muss auf Basis von Exchange 2010 oder neuer aufgesetzt sein.

Sie sollten außerdem auf allen Exchange Servern sämtliche verfügbaren Service Packs und Updates installieren. Denken Sie dabei auch an möglicherweise veröffentlichte *Update Rollups* oder *Cumulative Updates*.

▶ Domänenverifizierung

Im Microsoft 365-Mandanten müssen Sie vorab Ihre eigenen Domänen verifizieren.

▶ AutoErmittlung

Die AutoErmittlung muss eingerichtet sein.

▶ Zertifikate

Die Informationsdienste von CAS, Exchange Web Services und die AutoErmittlung müssen über ein öffentliches SSL-Zertifikat abgesichert sein. Ein selbst signiertes Zertifikat ist nicht ausreichend. Sind die URLs unterschiedlich, müssen sie als *SAN (Subject Alternative Name)* im Zertifikat hinterlegt sein – oder Sie nutzen ein Platzhalterzertifikat.

▶ Berechtigungen

Bei der Ausführung des Assistenten zur Hybridkonfiguration geben Sie die Benutzerkonten eines lokalen Exchange-Administrators und eines Exchange Online-Administrators ein. Beide müssen in der Rollengruppe *Organization Management* enthalten sein.

▶ Statische externe IP-Adresse

Verwenden Sie eine dynamische IP-Adresse an Ihrem Internetzugang (beispielsweise über die für privat angebotenen üblichen DSL-Anschlüsse), werden E-Mails von Ihrer lokalen Exchange-Organisation an Exchange Online höchstwahrscheinlich geblockt (Filterung auf IP-Basis über *Spamhaus*).

▶ Firewall

Ihre lokale Exchange-Umgebung muss über verschiedene Ports und Endpunkte aus dem Internet erreichbar sein. Tabelle 6.21 zeigt, welche Ports, Protokolle und Endpunkte davon betroffen sind.

| Port | Protokoll | Anwendung | Lokaler Endpunkt |
|-----------------|-------------------------------|---|---|
| TCP 25 (SMTP) | SMTP/TLS | Mailfluss zwischen Exchange Online und lokalem Exchange | <ul style="list-style-type: none"> ▶ Exchange 2019/2016: Postfach/EDGE ▶ Exchange 2013: CAS/EDGE ▶ Exchange 2010: HUB/EDGE |
| TCP 443 (HTTPS) | AutoDiscover (AutoErmittlung) | <ul style="list-style-type: none"> ▶ AutoDiscover (AutoErmittlung) ▶ OAuth | <ul style="list-style-type: none"> ▶ Exchange 2019/2016: Postfach ▶ Exchange 2013/2010: CAS |
| TCP 443 (HTTPS) | EWS | <ul style="list-style-type: none"> ▶ frei/gebucht ▶ E-Mail-Info ▶ Nachrichtenverfolgung ▶ postfachübergreifende Suche ▶ Postfachmigration ▶ OAuth | <ul style="list-style-type: none"> ▶ Exchange 2019/2016: Postfach ▶ Exchange 2013/2010: CAS |

Tabelle 6.19 Ports, Protokolle und Endpunkte

Achtung: Sowohl die Minimale Hybridkonfiguration als auch die Express-Hybridkonfiguration setzen voraus, dass die zu migrierenden Benutzer in Exchange Online noch kein Postfach haben. Möglicherweise haben Sie in Microsoft 365 bereits vor der Einrichtung der Verzeichnissynchronisierung Benutzerkonten angelegt und diese mit einer Exchange Online-Lizenz ausgestattet. In diesem Fall hat Microsoft 365 automatisch Postfächer angelegt. Eine Migration ist damit nicht mehr möglich. Entfernen Sie in diesem Fall die Postfächer in Exchange Online wieder (beispielsweise durch Lizenzentzug oder Löschen der Benutzerkonten – sofern das in diesem Stadium Ihrer aktuellen Konfiguration noch möglich ist).

E-Mail-Verkehr

Richten Sie eine dieser beiden Hybridkonfigurationen ein, nimmt während des Migrationszeitraums nach wie vor Ihre lokale Exchange-Organisation die E-Mails für Ihre Domäne entgegen. Liegt das Postfach eines Empfängers bereits in Exchange Online, werden entsprechende Mails von Ihrer lokalen Umgebung weitergeleitet.

Verschickt ein Benutzer, dessen Postfach bereits in Exchange Online liegt, eine neue E-Mail, wird sie von Exchange Online ohne Umweg über die lokale Umgebung direkt beim zuständigen E-Mail-Server ausgeliefert.

Migrationsvorgang

Der Migrationsvorgang lässt sich in folgende Schritte aufteilen:

1. Basiskonfiguration
2. Benutzerbereitstellung – diese ist abhängig davon, ob Sie eine dauerhafte Verzeichnissynchronisierung benötigen:
 - Variante »einmalige Benutzersynchronisierung«
 - Variante »dauerhafte Benutzersynchronisierung«
3. Benutzer lizenzieren
4. Postfächer migrieren
5. Ändern der DNS-Einträge

Sehen wir uns die Schritte nun im Einzelnen an.

Schritt 1: Basiskonfiguration

1. Für die spätere Synchronisierung der Benutzer müssen Sie zunächst im Mandanten die AAD-Synchronisierung freischalten. Stellen Sie dazu eine PowerShell-Verbindung her (siehe Abschnitt 3.14.3, »Azure Active Directory-Modul für Windows PowerShell«), und führen Sie dann das folgende Kommando aus:

```
Set-MSolDirSyncEnabled -EnableDirsync $true
```

Listing 6.54 AAD-Synchronisierung freischalten

2. Öffnen Sie auf einem Windows Server, der sich in derselben Domäne wie der lokale Exchange Server befindet, den Hybridkonfigurations-Assistenten unter der folgenden URL: <https://aka.ms/hybridwizard>

Damit wird der Hybridkonfigurations-Assistent heruntergeladen und gestartet (siehe Abbildung 6.111). Sollte es bei der Konfiguration zu einem Fehler kommen, können Sie den Assistenten später erneut starten. Dazu finden Sie nach dem ersten Start auf dem Desktop ein Anwendungssymbol.



Abbildung 6.111 Hybridkonfigurations-Assistent

3. Im Schritt **LOKALE EXCHANGE SERVER-ORGANISATION** versucht der Assistent nun automatisch, einen geeigneten Exchange Server ausfindig zu machen (siehe Abbildung 6.112). Sollte das nicht erfolgreich sein, geben Sie selbst einen Clientzugriffs-Server an. Außerdem geben Sie an, wo Ihr Mandant angelegt ist (im Normalfall **OFFICE 365 WORLDWIDE**).

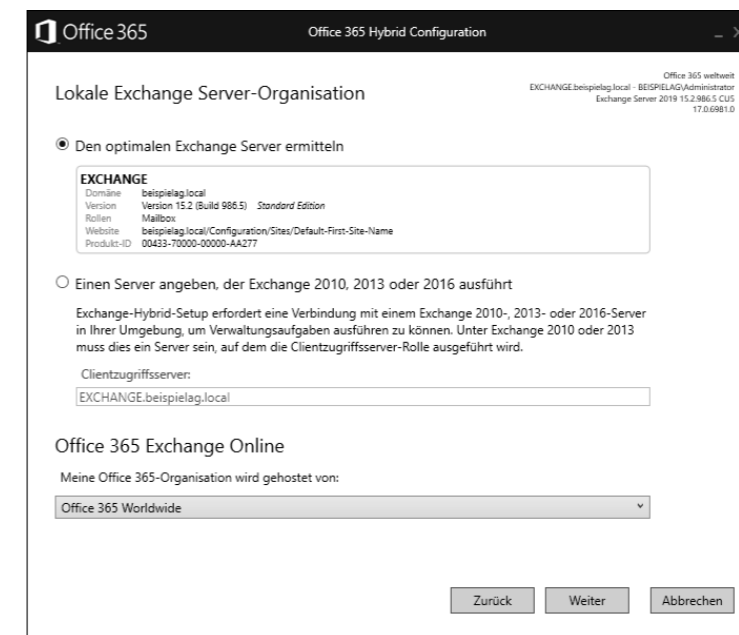


Abbildung 6.112 Lokale Exchange Server-Organisation

4. Im Schritt ANMELDEINFORMATIONEN geben Sie die Benutzerdaten eines lokalen Exchange- und eines Microsoft 365-Administrators an (siehe Abbildung 6.113).

Abbildung 6.113 Anmeldeinformationen

5. Im Schritt HYBRIDFUNKTIONEN entscheiden Sie sich wahlweise für die MINIMALE HYBRIDKONFIGURATION oder die VOLLSTÄNDIGE HYBRIDKONFIGURATION (siehe Abbildung 6.114). In diesem Abschnitt machen wir mit der Minimalen Hybridkonfiguration weiter, deren Ziel es ist, alle Postfächer zu Exchange Online zu transferieren. Die Vollständige Hybridkonfiguration beschreibe ich in Abschnitt 6.10, »Vollständige Exchange-Hybridkonfiguration«.
6. Im Schritt HYBRIDTOPOLOGIE wählen Sie die gewünschte Exchange-Konfiguration aus (siehe Abbildung 6.115). Im Beispiel verwende ich die KLASSISCHE EXCHANGE-HYBRIDTOPOLOGIE.
7. Im Schritt LOKALES KONTO FÜR MIGRATION geben Sie die Anmeldeinformationen für die lokale Exchange-Umgebung an, über die ein Migrationsendpunkt erzeugt wird (siehe Abbildung 6.116).
8. Nachdem Sie auf die Schaltfläche AKTUALISIEREN geklickt haben, nimmt der Assistent die erforderliche Konfiguration Ihrer lokalen Exchange-Umgebung und von Exchange Online vor. Dieser Vorgang kann einige Minuten in Anspruch nehmen.

Abbildung 6.114 Hybridfunktionen

Abbildung 6.115 Hybridtopologie

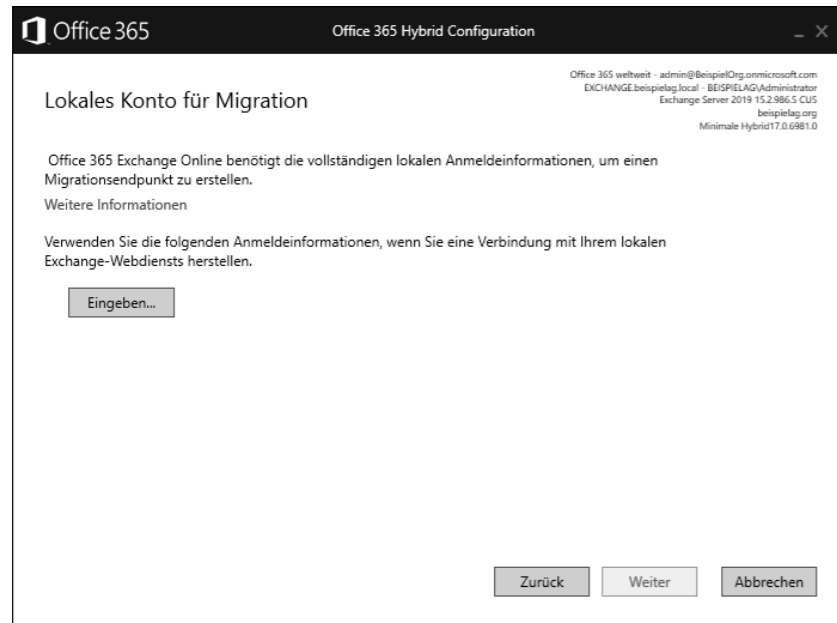


Abbildung 6.116 Lokales Konto für Migration

Schritt 2: Benutzerbereitstellung

Der Assistent fragt Sie nun im weiteren Verlauf, wie die lokal vorhandenen Benutzer in Microsoft 365 angelegt werden sollen. Dabei kommt das Verzeichnissynchronisierungstool AAD Connect zum Einsatz. Dieser Schritt wird übersprungen, wenn Sie die Active Directory-Verzeichnissynchronisierung bereits eingerichtet haben.

Im Schritt **BENUTZERBEREITSTELLUNG** entscheiden Sie sich, ob der Assistent selbst das Verzeichnissynchronisierungstool AAD Connect (siehe auch Abschnitt 4.2.1, »Verzeichnissynchronisierung«) installieren und konfigurieren soll oder ob Sie dies selbst vornehmen wollen (siehe Abbildung 6.117).

Die Option **MEINE BENUTZER UND KENNWÖRTER EINMALIG SYNCHRONISIEREN** führt dazu, dass AAD Connect nicht dauerhaft zum Einsatz kommt, sondern nur genau ein Mal, um die bestehenden lokalen Benutzer samt deren aktuellen Kennwörtern in Microsoft 365 anzulegen. Diese Option ist für kleine Umgebungen gedacht, die keine laufende Verzeichnissynchronisierung wünschen. Mit dieser Option entscheiden Sie sich also für die Express-Hybridkonfiguration. Mit der Option **ICH INSTALIERE ACTIVE DIRECTORY AZURE CONNECT SPÄTER SELBST** fahren Sie dagegen mit der Minimalen Hybridkonfiguration fort.



Mehr zu AAD Connect lesen Sie in Abschnitt 4.2.1, »Verzeichnissynchronisierung«.



Abbildung 6.117 Benutzerbereitstellung

Schritt 2 – Variante »Einmalige Benutzersynchronisierung«

Entscheiden Sie sich für diese Variante, wird die Installation von AAD Connect automatisch gestartet. Akzeptieren Sie die Lizenzbedingungen, und verwenden Sie die **EXPRESS-EINSTELLUNGEN** (siehe Abbildung 6.118).

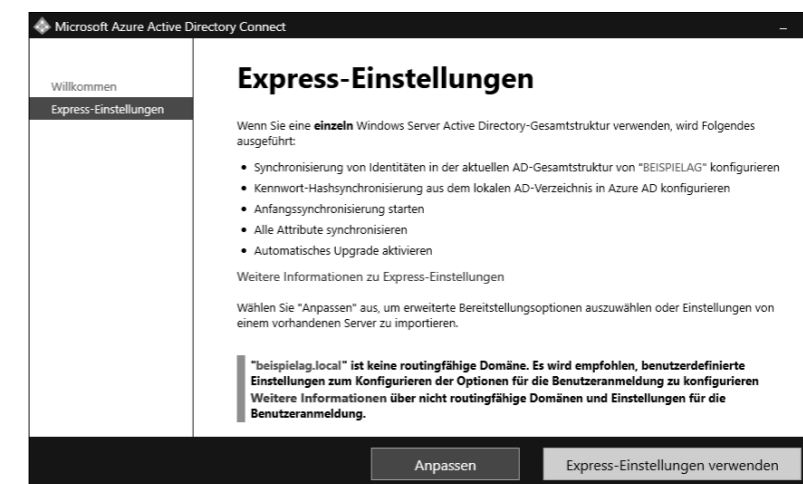


Abbildung 6.118 Konfiguration von AAD Connect

Alternativ dazu können Sie die Konfiguration von AAD Connect auch selbst anpassen, beispielsweise die zu synchronisierenden Benutzerkonten auswählen. Lesen Sie dazu Abschnitt 4.2.1, »Verzeichnissynchronisierung«.

Während der Konfiguration müssen Sie die Zugangsdaten eines Microsoft 365- und eines lokalen Domänenadministrators angeben.



Im Schritt **BEREIT ZUR KONFIGURATION** werden Sie gefragt, ob Sie eine Exchange-Hybridkonfiguration einrichten wollen. Aktivieren Sie diese Option nicht, denn sie ist nur für die vollständige Hybridkonfiguration erforderlich.

Nach der Installation von AAD Connect wird die Synchronisierung genau ein Mal durchgeführt, und anschließend wird sie automatisch deaktiviert. AAD Connect selbst wird jedoch nicht automatisch deinstalliert. Sie müssen das selbst über die Systemsteuerung vornehmen.

Schritt 2 – Variante »Dauerhafte Benutzersynchronisierung«

Entscheiden Sie sich dafür, AAD Connect später zu installieren, ist der Assistent damit beendet, und Sie können sich an die eigenständige Konfiguration von AAD Connect machen. Die Option **EXCHANGE-HYBRIDEINSTELLUNG** im Konfigurationsassistent von AAD Connect aktivieren Sie nicht, da sie nur bei der vollständigen Hybridkonfiguration erforderlich ist.

Nachdem Sie AAD Connect eingerichtet haben, können Sie mit dem nächsten Schritt weitermachen.

Schritt 3: Benutzer lizenzieren

Bevor Sie mit der Migration der Postfachinhalte fortfahren können, müssen Sie die Benutzerkonten in Microsoft 365 mit einer Lizenz ausstatten, die Exchange Online beinhaltet. Dieser Schritt wird nicht automatisch gemacht. Die Varianten der Lizenzierung finden Sie in Abschnitt 2.5.2, »Benutzer anlegen«, beschrieben.

Schritt 4: Postfächer migrieren

Im nächsten Schritt folgt die eigentliche Migration der Postfachinhalte:

1. Im EAC von Exchange Online wechseln Sie zum Bereich **EMPFÄNGER** und dort zum Abschnitt **MIGRATION** (siehe Abbildung 6.119).
2. Klicken Sie auf **MIGRATIONSbatch HINZUFÜGEN**, erscheint der E-Mail-Migrations-Assistent (siehe Abbildung 6.120).
3. Geben Sie einen Namen für den Migrationsbatch ein, und wählen Sie als **POSTFACH-MIGRATIONSPFAD** die Option **MIGRATION ZU EXCHANGE ONLINE**.

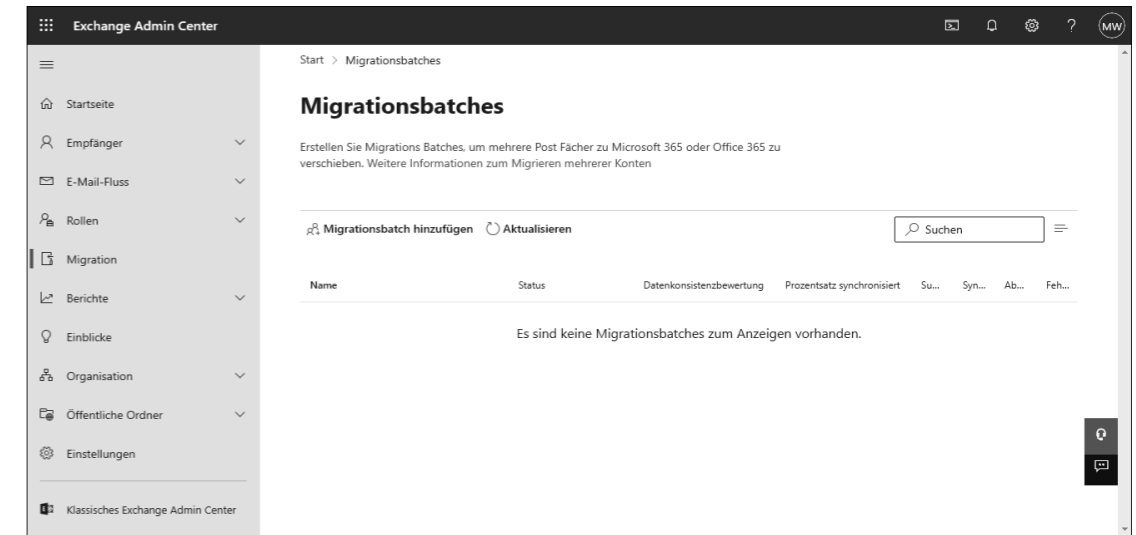


Abbildung 6.119 Der Migrations-Bereich im EAC

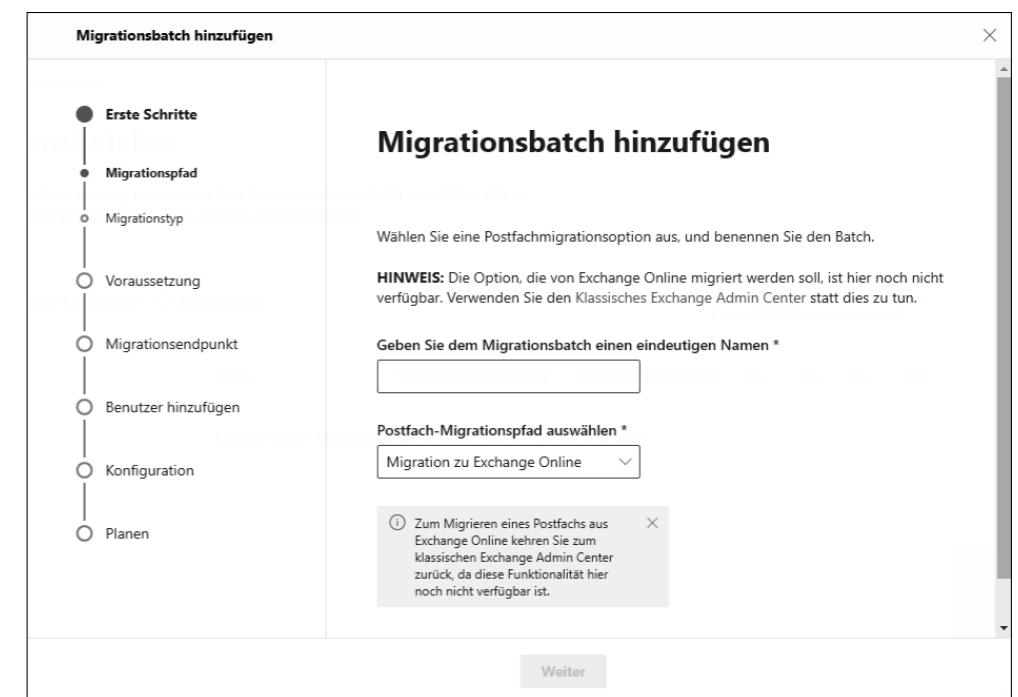


Abbildung 6.120 Der E-Mail-Migrations-Assistent

4. Im Schritt **MIGRATIONSTYP** wählen Sie die Option **REMOTE-VERSCHIEBUNGSMIGRATION** (siehe Abbildung 6.121).

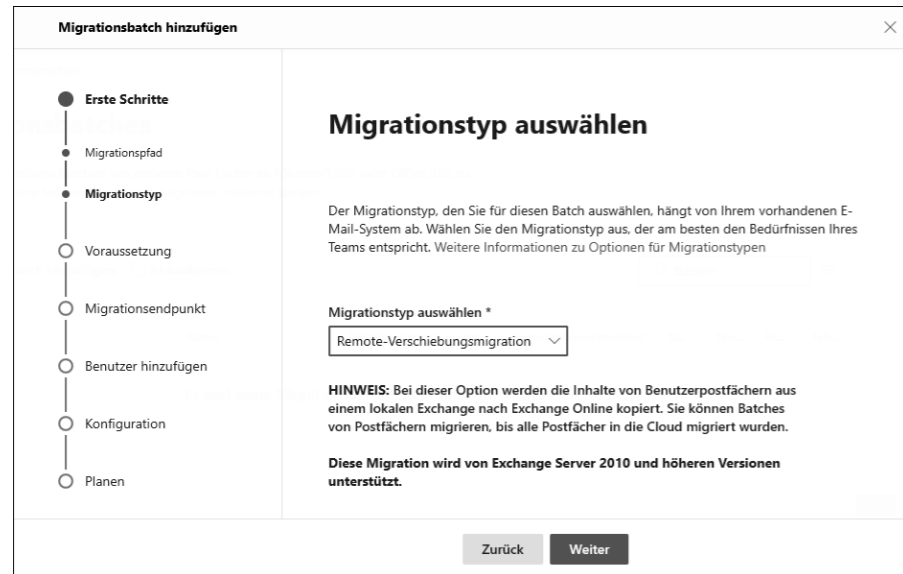


Abbildung 6.121 Migrationstyp

5. Lesen und beachten Sie im Schritt VORAUSSETZUNGEN die Hinweise (siehe Abbildung 6.122).

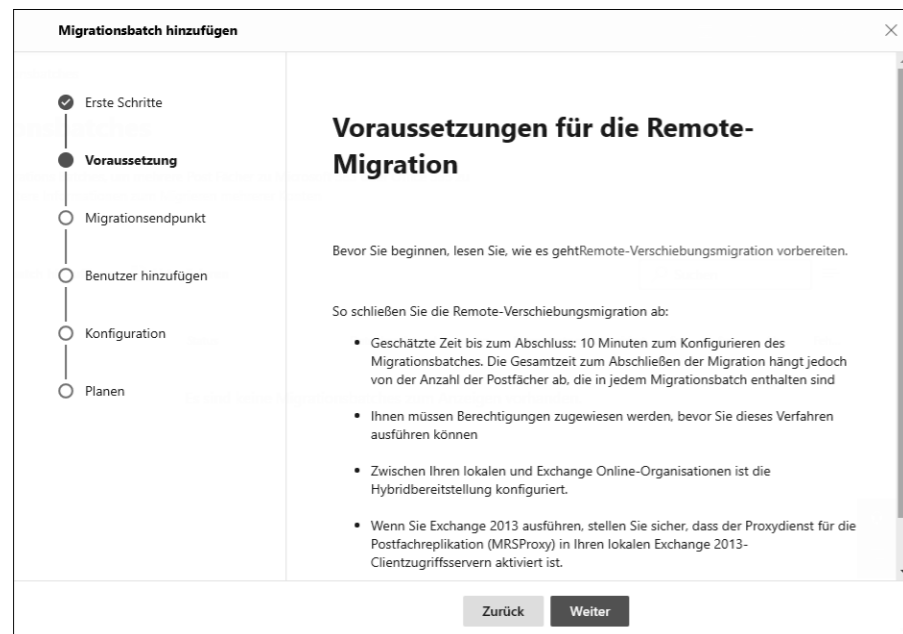


Abbildung 6.122 Voraussetzungen

6. Im Schritt MIGRATIONSENDPUNKT wählen Sie HYBRID MIGRATION ENDPOINT aus (siehe Abbildung 6.123). Der Migrationsendpunkt wurde bei der Einrichtung vom Hybrid-Konfigurationsassistenten erstellt.

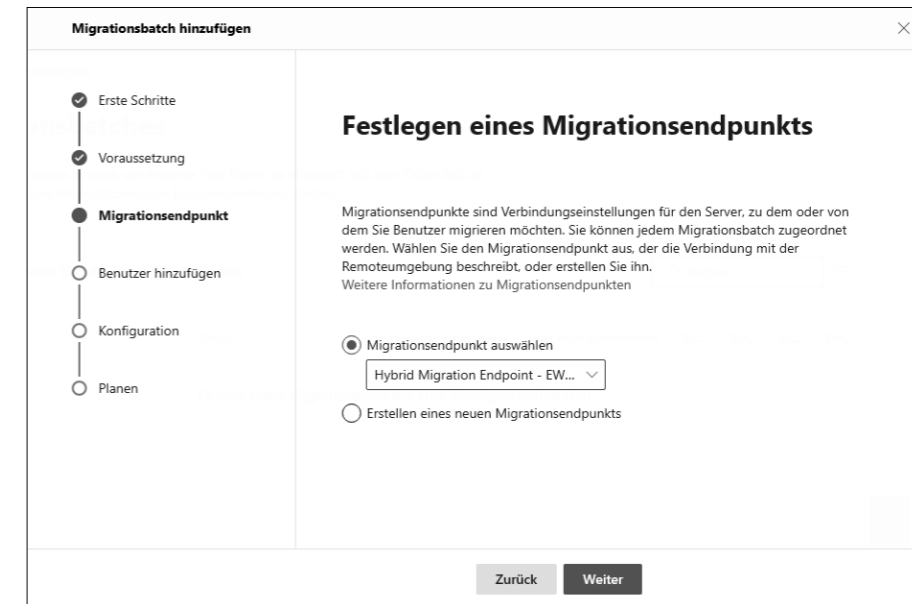


Abbildung 6.123 Migrationsendpunkt

7. Wählen Sie im Schritt BENUTZER HINZUFÜGEN die zu verschiebenden Benutzer aus, oder laden Sie eine CSV-Datei mit den E-Mail-Adressen der zu verschiebenden Benutzer hoch (siehe Abbildung 6.124).

Die CSV-Datei legen Sie mit der Spalte `EmailAddress` an und hinterlegen in jeder Zeile eine E-Mail-Adresse.

Sollte in der Benutzerauswahlliste ein Benutzer mit lokalem Postfach nicht enthalten sein, liegt das möglicherweise daran, dass für den Benutzer bereits ein Exchange Online-Postfach existiert. Damit ist das Verschieben des lokalen Postfachs nicht möglich. Diese Situation kann auftreten, wenn Sie vor der Aktivierung der Exchange-Hybridkonfiguration im Verzeichnissynchronisierungstool dem Benutzer eine Exchange Online-Lizenz zugewiesen haben. Damit wird automatisch ein Exchange Online-Postfach angelegt. Das geschieht aber nicht, wenn im Verzeichnissynchronisierungstool die Hybridkonfiguration aktiviert ist und der Benutzer bereits über ein lokales Postfach verfügt.

8. Im Schritt KONFIGURATION geben Sie die ZIELZUSTELLUNGSDOMÄNE an (siehe Abbildung 6.125). Achtung: Geben Sie hier nicht (!) Ihre eigene Domäne an, sondern die Domäne mit der Endung `mail.onmicrosoft.com`.

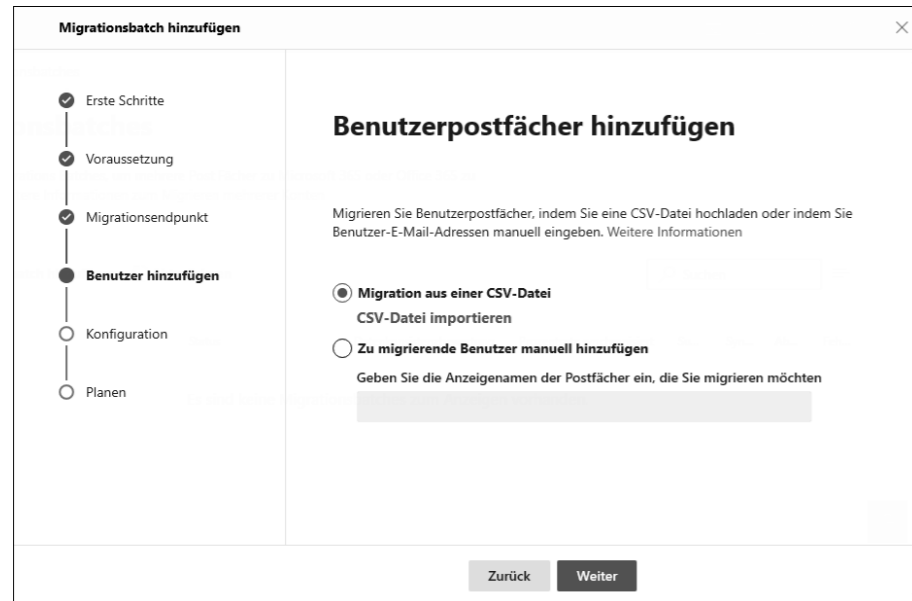


Abbildung 6.124 Benutzer hinzufügen

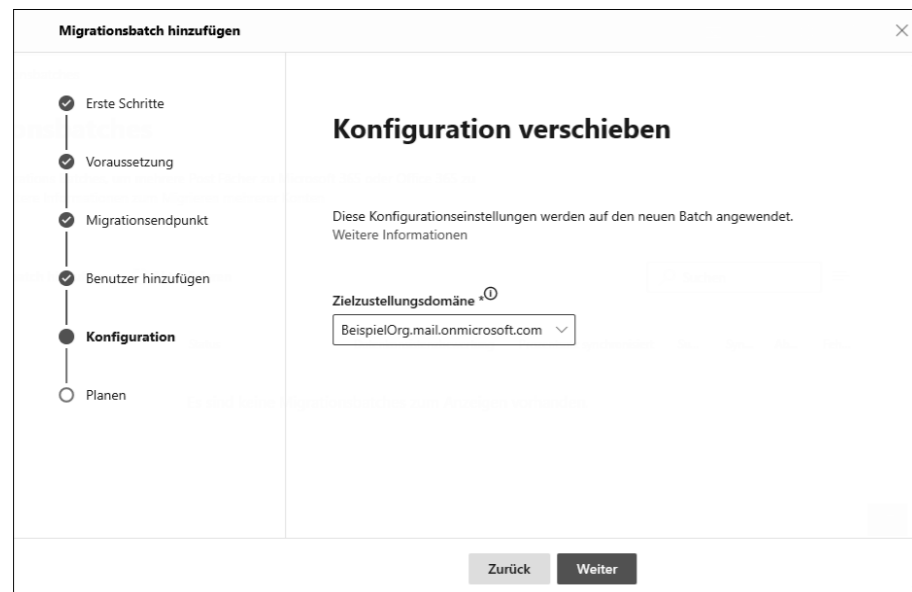


Abbildung 6.125 Konfiguration

9. Im letzten Schritt, PLANEN, geben Sie einen Microsoft 365-Benutzer an, der über den Fortschritt der Migration per E-Mail benachrichtigt wird. Außerdem entscheiden Sie, ob die Migration unmittelbar oder zu einem späteren Zeitpunkt begonnen werden soll. Die

Option Batch automatisch starten wählen Sie, um dies nicht selbst nach dem Verschiebevorgang tun zu müssen (siehe Abbildung 6.126).

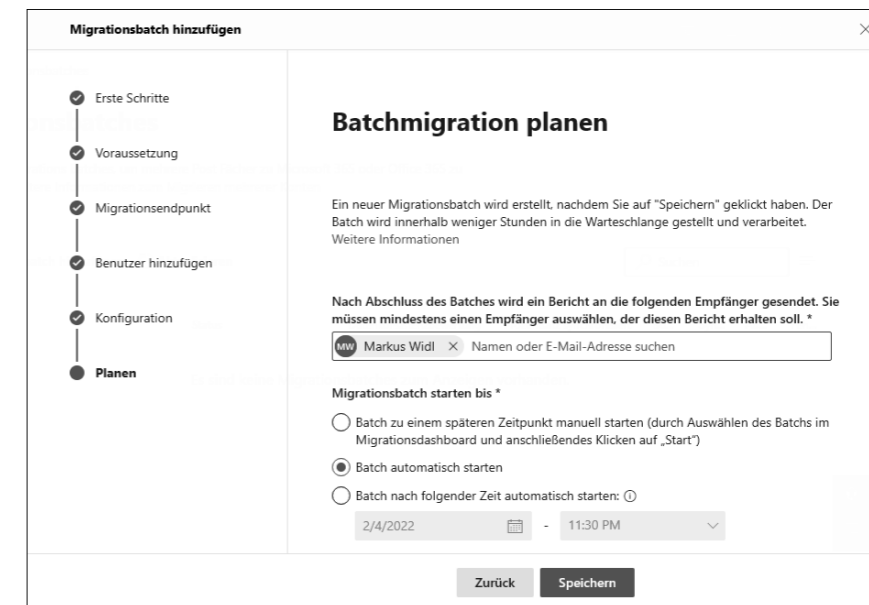


Abbildung 6.126 Planen

10. Damit schließen Sie den Assistenten. Das EAC zeigt den neuen Migrationsbatch an (siehe Abbildung 6.127).

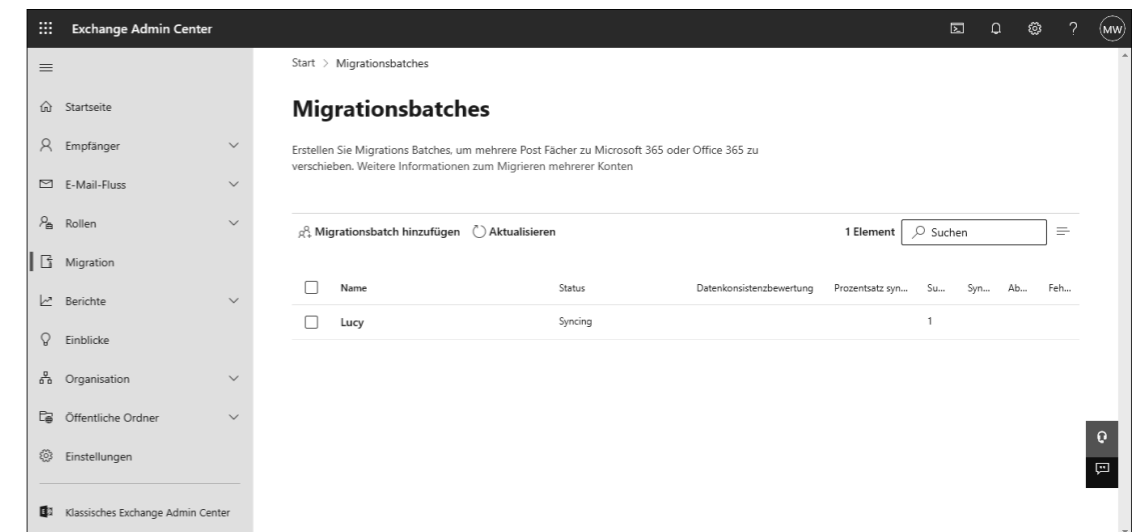


Abbildung 6.127 Migrationsfortschritt

11. Falls Sie sich für einen späteren Start der Migration entschieden haben, markieren Sie den Migrationsbatch und klicken auf die Schaltfläche **MIGRATION STARTEN**, um mit der Migration zu beginnen.

Schritt 4: Ändern der DNS-Einträge

Nachdem alle erforderlichen Postfächer migriert wurden, ändern Sie die Einträge *MX*, *Auto-Ermittlung* sowie *SPF* in den Einstellungen Ihres DNS-Anbieters entsprechend den Vorgaben von Microsoft 365.

Danach sollten Sie warten, bis sich die Änderung in der DNS-Infrastruktur verbreitet hat. Dies kann bis zu drei Tage dauern. Wie die DNS-Einträge aussehen sollen, können Sie in Abschnitt 2.4.2, »Domäne verifizieren«, nachlesen.

»] Vergessen Sie dabei nicht Ihren internen DNS-Server, sofern dort auch ein AutoErmittlungseintrag vorhanden ist. Ansonsten bekommen die internen Clients Probleme bei der Verbindung mit Exchange Online, da sie sich nach wie vor bei der alten Umgebung anmelden.

»] Wollen Sie den oder die bestehenden Exchange Server nach einer erfolgreichen Migration abschalten, sind vorab noch einige Aufräumarbeiten erforderlich, die von der aktuellen Konfiguration abhängen. Eine gute Übersicht finden Sie hier:

<https://docs.microsoft.com/de-de/exchange/decommission-on-premises-exchange>

6.10 Vollständige Exchange-Hybridkonfiguration

Bei einer Vollständigen Hybridkonfiguration betreiben Sie neben Exchange Online dauerhaft eine lokale Exchange Server-Umgebung weiter (im weiteren Verlauf dieses Abschnitts schreibe ich zur Vereinfachung statt »vollständige Hybridkonfiguration« nur noch »Hybridkonfiguration«). Dabei sollen diese beiden separaten Organisationen, zumindest für den Endanwender als eine einzelne Organisation angesehen werden. Hilfreiche Funktionen, wie beispielsweise die Anzeige der Verfügbarkeitsinformationen, sollen für alle Anwender, egal in welcher Organisation sie ihr Postfach haben, nach wie vor funktionieren.

Eine Hybridkonfiguration eignet sich unter anderem für die folgenden Szenarien:

► **Sensible Postfächer bleiben lokal**

Sie wollen zwar grundsätzlich von den günstigen Konditionen der Exchange Online-Lizenzen profitieren und einen Teil der Speicherkosten für die Verwaltung von lokalen Postfächern einsparen, aber sensible Postfächer dennoch weiterhin lokal betreiben. Zu diesen Postfächern könnten beispielsweise die Postfächer der Geschäftsführung oder der Entwicklungsabteilung gehören. Während diese lokal bleiben, werden die Postfächer der anderen Anwender in Exchange Online abgelegt.

► **Viele Außendienstmitarbeiter**

Ihre Außendienstmitarbeiter sind viel unterwegs. Ihre Internetanbindung lässt aber zu wünschen übrig, sodass die Arbeit mit Ihrer Exchange-Umgebung zum Geduldsspiel wird. Liegen die Postfächer der Außendienstmitarbeiter in Exchange Online, entlasten Sie Ihre Internetanbindung.

► **Archivpostfächer in Exchange Online**

Sie wollen zwar die Archivpostfach-Funktionalität von Exchange einsetzen, aber die enormen Kosten für die erforderliche lokale Speicherkapazität einsparen. Die primären Postfächer selbst sollen aber nach wie vor lokal betrieben werden. Für dieses Szenario gibt es sogar eine eigene Lizenz, die es Ihnen kostengünstig ermöglicht, nur die Archivpostfächer in Exchange Online zu betreiben (siehe dazu auch Abschnitt 6.1.2, »Lizenzüberblick«).

In diesem Abschnitt werden wir uns mit der Hybridkonfiguration auf Basis des Exchange Servers 2019 beschäftigen. Das heißt aber nicht, dass eine Hybridkonfiguration mit einer Exchange-Umgebung auf einer älteren Version nicht funktioniert. Grundsätzlich können Sie ab Exchange 2010 eine Hybridkonfiguration einrichten. Vor der Konfiguration sollten Sie jedoch sicherstellen, dass jeweils das neueste *CU (Cumulative Update)* oder *UR (Update Rollup)* installiert wurde, um möglichen Problemen vorzubeugen.

Außerdem werden wir wieder gelegentlich mit der PowerShell arbeiten, diesmal allerdings nicht primär mit der Erweiterung für Exchange Online, sondern mit der des Exchange Servers. Für die Verwaltung Ihrer lokalen Exchange-Organisation führen Sie also die *Exchange Management Shell (EMS)* aus dem Startmenü bzw. von der Startseite aus. Wollen Sie dagegen mit den in Exchange Online angelegten Postfächern arbeiten, verbinden Sie sich wie bisher mit Exchange Online. Ist es erforderlich, dass Sie parallel mit beiden Organisationen arbeiten, lohnt sich der Import der Exchange Online-Erweiterung mit einem alternativen Präfix, um keine Namenskollisionen bei den Cmdlets zu erhalten. Lesen Sie hierzu Abschnitt 6.3.3, »Verbindungsaufbau«.

6.10.1 E-Mail-Verkehr

Im Regelfall verwenden Sie bei einer Hybridkonfiguration einen geteilten Namensraum. Das heißt, Sie benutzen dieselbe Domäne (beispielsweise *beispielag.de*) für Postfächer beider Organisationen. Außerdem dürfte zumindest zu Beginn der Einrichtung der MX-Eintrag Ihrer Domäne auf die lokale Organisation zeigen. Die Frage ist nun, wie E-Mails zwischen den Organisationen ausgetauscht werden, um dann im jeweiligen Zielpostfach anzukommen.

Dabei stehen Ihnen mehrere Optionen zur Auswahl. Außerdem müssen wir den eingehenden und ausgehenden E-Mail-Verkehr separat betrachten.

Eine wichtige Information noch vorab: Im Rahmen der Einrichtung einer Hybridkonfiguration wird eine sogenannte *Hybriddomäne* eingerichtet. Diese trägt den folgenden Namen:

MANDANTDOMÄNE.mail.onmicrosoft.com

Die Hybriddomäne wird bei allen E-Mail-Adressrichtlinien als sekundäre Proxydomäne eingetragen. Ihre Bedeutung wird gleich ersichtlich.

Die Kommunikation zwischen den beiden Exchange-Organisationen wird dabei standardmäßig über *TLS* abgesichert.

Eingehende E-Mails mit der lokalen Organisation empfangen

Nehmen wir an, der MX-Eintrag der Domäne *beispielag.de* zeigt auf die lokale Organisation. Eine E-Mail wird an *lucy@beispielag.de* sowie an *robin@beispielag.de* geschickt, wobei Robins Postfach in der lokalen Organisation und Lucys Postfach in Exchange Online liegt.

Die Verarbeitung dieser E-Mail sieht dann wie folgt aus (siehe Abbildung 6.128).

- ❶ Die E-Mail trifft beim Clientzugriffs-Server der lokalen Exchange-Umgebung ein.
- ❷ Da die E-Mail an ein lokales Postfach gerichtet ist (Robin), wird sie entsprechend ausgeliefert. Da aber ebenso ein Exchange Online-Postfach betroffen ist (Lucy), wird die E-Mail vom Clientzugriffs-Server mithilfe der Hybriddomäne (*beispielag.mail.onmicrosoft.com*) und eines entsprechend konfigurierten Sendecollectors zu EOP von Exchange Online weitergeleitet.
- ❸ EOP überprüft den Inhalt der E-Mail (Spam, Schadcode etc.).
- ❹ Anschließend wird die E-Mail in das Zielpostfach abgelegt.

Etwas anders sieht der Vorgang aus, wenn der MX-Eintrag auf Exchange Online zeigt und nicht auf die lokale Organisation.

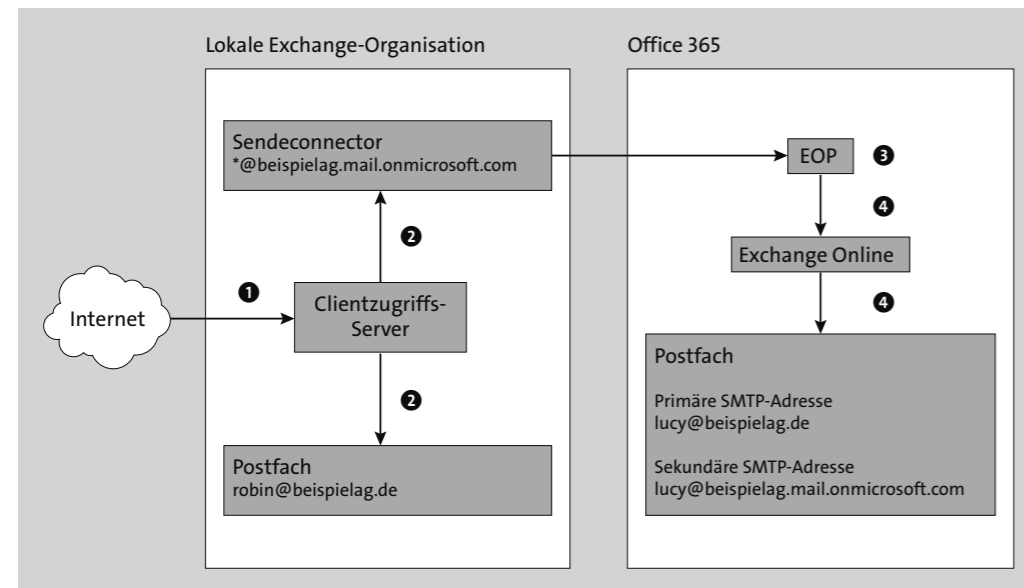


Abbildung 6.128 Eingehende E-Mails mit der lokalen Organisation empfangen

Eingehende E-Mails mit Exchange Online empfangen

Beim Empfang eingehender E-Mails mit Exchange Online gibt es eine Option, die Sie berücksichtigen müssen: Beim Einrichten einer Hybridkonfiguration haben Sie die Wahl, ob der *zentrale E-Mail-Transport* aktiviert werden soll. Standardmäßig ist er das nicht. Aktivieren Sie ihn, stellen Sie damit sicher, dass alle eingehenden E-Mails auf jeden Fall über Ihre lokale Exchange-Organisation geleitet werden. Warum Sie das tun sollten? Möglicherweise betreiben Sie lokal eine Vorrichtung, die sämtlichen E-Mail-Verkehr zur Archivierung oder gesetzlich vorgeschriebenen Aufbewahrung protokolliert. Indem Sie den zentralen E-Mail-Transport aktivieren, stellen Sie dabei sicher, dass auch E-Mails an Exchange Online-Postfächer berücksichtigt werden. Natürlich wäre es auch eine Option, den MX-Eintrag dann eben nicht auf Exchange Online zeigen zu lassen, sondern auf die lokale Organisation. Ein Vorteil geht dann allerdings verloren: Zeigt der MX-Eintrag auf Exchange Online, werden alle eintreffenden E-Mails von EOP auf unerwünschte Inhalte hin untersucht und gegebenenfalls ausgefiltert – eben auch die E-Mails, die für lokale Postfächer bestimmt sind. Damit sparen Sie sich möglicherweise andere Lösungen zur E-Mail-Hygiene.

Achtung: Verwenden Sie EOP für lokale Postfächer, sind gegebenenfalls entsprechende Lizenzen erforderlich. Diese können Sie in Ihrem Microsoft 365-Mandanten zusätzlich buchen. [<<]

Betrachten wir zunächst den Standardfall, bei dem der zentrale E-Mail-Transport nicht aktiviert ist. Auch hier nutzen wir wieder das Beispiel: Eine E-Mail wird an *lucy@beispielag.de* sowie an *robin@beispielag.de* geschickt. Robins Postfach ist lokal, Lucys in Exchange Online. Sehen Sie sich hierzu Abbildung 6.129 an.

- ❶ EOP empfängt die E-Mail, überprüft den Inhalt und leitet sie an Exchange Online weiter.
- ❷ Exchange Online erkennt einen der Empfänger mit einem Cloudpostfach (Lucy) und einen mit lokalem Postfach (Robin). Lucys Kopie der E-Mail wird ausgeliefert.
- ❸ Robins E-Mail wird wieder zurück zu EOP gesandt.
- ❹ EOP leitet die E-Mail weiter an den Clientzugriffs-Server der lokalen Organisation. Die E-Mail wird anschließend ausgeliefert.

Und jetzt der gleiche Vorgang mit aktiviertem zentralen E-Mail-Transport (siehe Abbildung 6.130).

- ❶ EOP empfängt die E-Mail und überprüft den Inhalt.
- ❷ Die E-Mail wird zunächst an den Clientzugriffs-Server der lokalen Organisation weitergeleitet.
- ❸ Robins E-Mail wird in sein Postfach ausgeliefert.
- ❹ Eine Kopie der Mail wird für Lucy zurück an EOP gesandt.
- ❺ EOP leitet die Mail weiter an Exchange Online.
- ❻ Exchange Online liefert Lucys E-Mail aus.

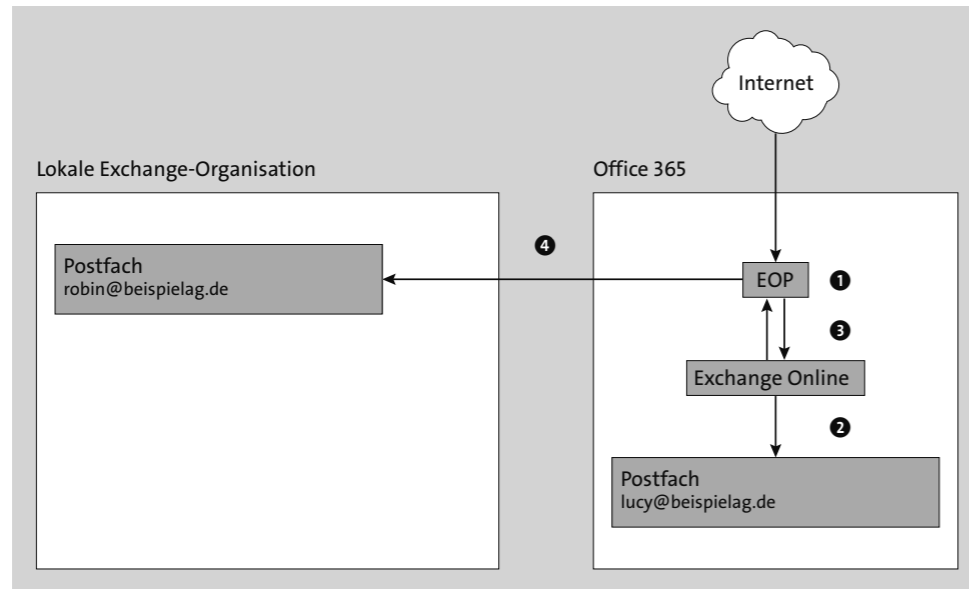


Abbildung 6.129 Eingehende E-Mails mit Exchange Online ohne zentralen E-Mail-Transport empfangen

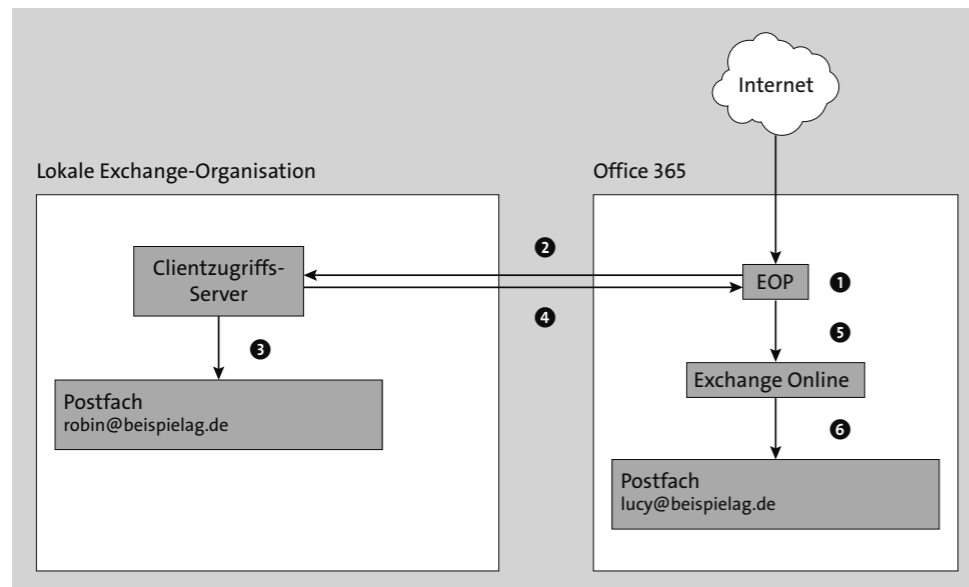


Abbildung 6.130 Eingehende E-Mails mit Exchange Online mit zentralem E-Mail-Transport empfangen

Nachdem wir jetzt den eingehenden E-Mail-Verkehr betrachtet haben, kümmern wir uns nun um die Gegenrichtung.

Ausgehender E-Mail-Verkehr

Betrachten wir den Vorgang, wenn eine E-Mail von einem Exchange Online-Postfach an einen externen Empfänger versandt wird. Auch beim ausgehenden E-Mail-Verkehr wird dabei zwischen aktiviertem und deaktiviertem zentralem E-Mail-Transport unterschieden.

Ist er deaktiviert (Standard), erfolgt der Versand wie folgt (siehe Abbildung 6.131):

- ❶ Die E-Mail wird zu EOP geschickt und dort inhaltlich überprüft.
- ❷ Die E-Mail wird direkt beim zuständigen E-Mail-Server ausgeliefert.

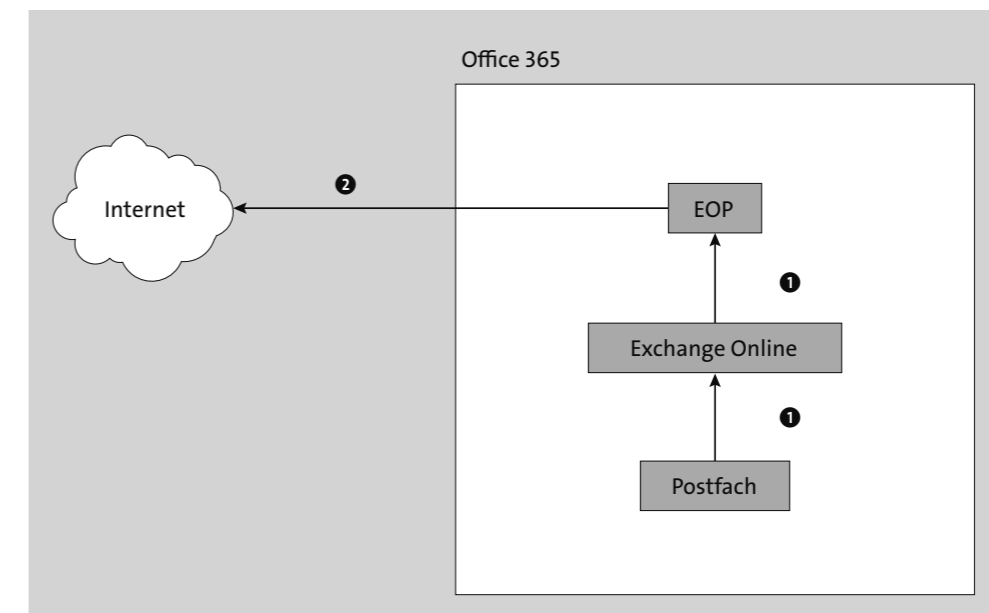


Abbildung 6.131 Ausgehende E-Mail ohne zentralen E-Mail-Transport

Das war jetzt nicht besonders schwierig. Deutlich aufwendiger ist der Vorgang bei aktiviertem zentralem E-Mail-Transport (siehe Abbildung 6.132).

- ❶ Die E-Mail wird zu EOP geschickt und dort inhaltlich überprüft.
- ❷ Die E-Mail wird zum Clientzugriffs-Server der lokalen Organisation weitergeleitet.

- ❸ Die E-Mail wird entsprechend der lokalen Konfiguration verarbeitet.

Das könnte ein zusätzlicher Inhaltscheck sein oder, wie bereits angesprochen, die Archivierung etc.

- ❹ Die E-Mail wird beim zuständigen E-Mail-Server ausgeliefert.



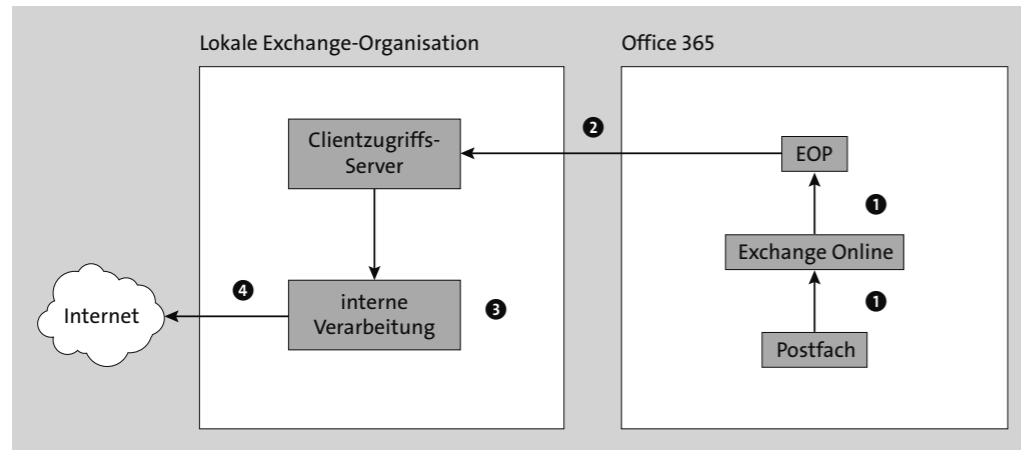


Abbildung 6.132 Ausgehende E-Mail mit zentralem E-Mail-Transport

6.10.2 Besonderheiten bei Berechtigungen

In einer Exchange-Hybridkonfiguration müssen Sie einige Besonderheiten im Zusammenhang mit Postfachberechtigungen berücksichtigen:

► Übergreifende Berechtigungen zwischen lokalen Postfächern und Exchange Online-Postfächern

Bei diesem Szenario müssen Sie zwischen verschiedenen Berechtigungstypen unterscheiden. Geben Sie einem lokalen Postfach *Vollzugriffsberechtigungen* auf ein Postfach in Exchange Online – oder umgekehrt –, funktioniert dies in einer Hybridkonfiguration. Dagegen funktioniert dies nicht mit den Berechtigungstypen *Senden als* und *Senden im Auftrag*.

► Berechtigungen beim Verschieben eines Postfachs zu Exchange Online

Berechtigungen der Typen *Vollzugriff*, *Senden als* und *Senden im Auftrag* werden beim Verschieben eines Postfachs im Rahmen einer Hybridkonfiguration mit verschoben, sofern die Berechtigungen direkt auf das Postfach angewandt wurden.

6.10.3 Voraussetzungen

Bevor Sie eine Hybridkonfiguration für Ihre primäre Umgebung umsetzen, sollten Sie diesen Vorgang anhand einer abgeschlossenen Testumgebung üben. Mithilfe von Exchange 2013 und 2016 ist es zwar im Vergleich zu den Vorversionen einfacher geworden, es ist aber immer noch ein komplexer Vorgang. Es wäre fatal, wenn Sie im Prozess merken sollten, dass E-Mails nicht mehr ankommen oder ausgeliefert werden.

Die Voraussetzungen für eine Hybridkonfiguration sind die folgenden:

► Exchange-Version

Die lokale Exchange-Umgebung muss für eine Hybridkonfiguration geeignet sein. Falls erforderlich, erhalten Sie über den Microsoft 365-Kundendienst (siehe Abschnitt 2.9.5, »Serviceanfragen«) eine Lizenz für den bei älteren Exchange-Versionen erforderlichen Exchange 2010. Sie sollten außerdem auf allen Exchange Servern sämtliche verfügbaren Service Packs und Updates installieren. Denken Sie dabei auch an möglicherweise veröffentlichte *Update Rollups* oder *Cumulative Updates*.

► Domänenverifizierung

Im Microsoft 365-Mandanten müssen Sie vorab Ihre eigenen Domänen verifizieren. Eine Hybridkonfiguration nur mit der initialen *onmicrosoft.com*-Domäne ist nicht möglich.

► Active Directory-Synchronisierung

Die Active Directory-Synchronisierung muss bereits eingerichtet sein. Wichtig ist, dass Sie während der Synchronisierungskonfiguration mit dem Assistenten die hybride Exchange-Bereitstellung aktiviert haben (siehe Abbildung 6.133). Haben Sie das nicht gemacht, führen Sie den Assistenten erneut aus (siehe Abschnitt 4.3.4, »Installation und Konfiguration«).

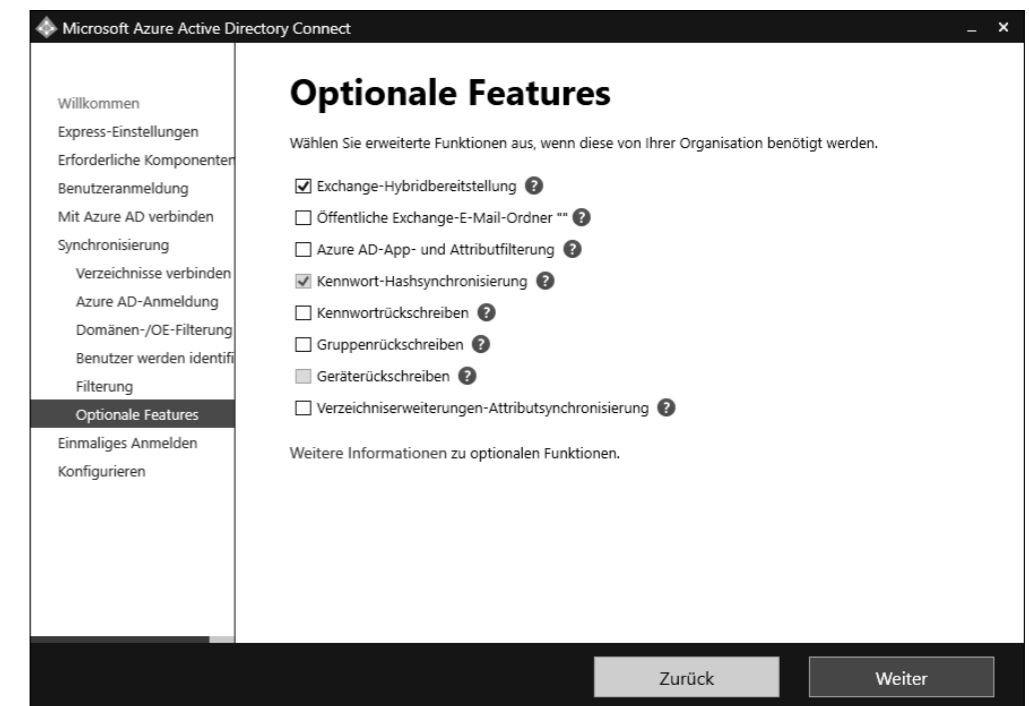


Abbildung 6.133 Aktivierung der Hybridkonfiguration in der Active Directory-Synchronisierung

Mit der Aktivierung erlauben Sie dem Synchronisierungstool, das für die Hybridkonfiguration erforderlich ist, diverse Attribute in Ihrem lokalen Active Directory zu ändern. Tabelle 6.20 führt für Sie die betroffenen Attribute auf.

Mit der Aktivierung der hybriden Exchange-Bereitstellung ändert sich auch das Verhalten bei der Lizenzzuweisung: Verfügt ein Benutzer bereits über ein lokales Postfach, erhält er durch die Zuweisung einer Exchange Online-Lizenz nicht mehr automatisch ein Exchange Online-Postfach. Das hat auch seinen guten Grund, denn ansonsten könnte das lokale Postfach nicht mehr zu Exchange Online verschoben werden, weil dort ja bereits ein Postfach für den Benutzer vorhanden ist.

| Exchange-Funktion | Beschriebenes Attribut |
|--|---|
| Filterung von sicheren und blockierten Absendern | msExchBlockedSendersHash msExchSafeRecipientsHash msExchSafeSendersHash |
| Archivierung in Exchange Online | msExchArchiveStatus msExchUserHoldPolicies |
| E-Mail-Fluss zwischen den Exchange-Umgebungen | proxyAddresses |
| SendOnBehalfTo-Rechte für Cloudbenutzer auf lokales Postfach | publicDelegates |
| Exchange Unified Messaging mit Microsoft Lync Server-Integration | msExchUCVoiceMailSettings |
| Exchange 2019/2016 | msDS-ExternalDirectoryObjectID |

Tabelle 6.20 Active Directory-Attribute

► **AutoErmittlung**

Die AutoErmittlung muss eingerichtet sein.

► **Zertifikate**

Die Informationsdienste von CAS, Exchange Web Services und die AutoErmittlung müssen über ein öffentliches SSL-Zertifikat abgesichert sein. Ein selbst signiertes Zertifikat ist nicht ausreichend. Sind die URLs unterschiedlich, müssen sie als SAN (*Subject Alternative Name*) im Zertifikat hinterlegt sein – oder Sie nutzen ein Platzhalterzertifikat.

► **Berechtigungen**

Bei der Ausführung des Assistenten zur Hybridkonfiguration geben Sie die Benutzerkonten eines lokalen Exchange-Administrators und eines Exchange Online-Administrators ein. Beide müssen in der Rollengruppe *Organization Management* enthalten sein.

► **Statische externe IP-Adresse**

Verwenden Sie eine dynamische IP-Adresse an Ihrem Internetzugang (beispielsweise über die für privat angebotenen üblichen DSL-Anschlüsse), werden E-Mails von Ihrer lokalen Exchange-Organisation an Exchange Online höchstwahrscheinlich geblockt (Filterung auf IP-Basis über *Spamhaus*).

► **Firewall**

Ihre lokale Exchange-Umgebung muss über verschiedene Ports und Endpunkte aus dem Internet erreichbar sein. Tabelle 6.21 zeigt, welche Ports, Protokolle und Endpunkte davon betroffen sind.

| Port | Protokoll | Anwendung | Lokaler Endpunkt |
|-----------------|-------------------------------|---|---|
| TCP 25 (SMTP) | SMTP/TLS | Mailfluss zwischen Exchange Online und lokalem Exchange | <ul style="list-style-type: none"> ► Exchange 2019/2016: Postfach/EDGE ► Exchange 2013: CAS/EDGE ► Exchange 2010: HUB/EDGE |
| TCP 443 (HTTPS) | AutoDiscover (AutoErmittlung) | <ul style="list-style-type: none"> ► AutoDiscover (AutoErmittlung) ► OAuth | <ul style="list-style-type: none"> ► Exchange 2019/2016: Postfach ► Exchange 2013/2010: CAS |
| TCP 443 (HTTPS) | EWS | <ul style="list-style-type: none"> ► frei/gebucht ► E-Mail-Info ► Nachrichtenverfolgung ► postfachübergreifende Suche ► Postfachmigration ► OAuth | <ul style="list-style-type: none"> ► Exchange 2019/2016: Postfach ► Exchange 2013/2010: CAS |

Tabelle 6.21 Ports, Protokolle und Endpunkte

Ist eine dieser Voraussetzungen nicht erfüllt, werden Sie die Assistenten zur Hybridkonfiguration nicht durchlaufen können, oder es wird im Anschluss daran Probleme beim E-Mail-Verkehr geben.

Die Einrichtung eines Identitätsverbunds für Single Sign-on ist dagegen keine Voraussetzung für eine Hybridkonfiguration, auch wenn sie in diesem Szenario empfohlen wird.

6.10.4 Testumgebung einrichten

Wollen Sie eine Hybridkonfiguration testen, haben Sie vermutlich bereits einen einzelnen, möglichst aktuellen Exchange Server in der Standardkonfiguration aufgesetzt. Ich verwende in diesem Abschnitt einen Exchange Server 2019.

Stellen Sie sicher, dass Sie die Voraussetzungen aus Abschnitt 6.10.3 dabei erfüllt haben, also beispielsweise eine eigene Domäne verifiziert, die Active Directory-Synchronisierung aktiviert haben etc. Diesen einzelnen Exchange-Server könnten Sie dann wie folgt konfigurieren (wohlgemerkt: für eine Testumgebung).

Akzeptierte Domäne

Falls es noch nicht geschehen ist, hinterlegen Sie die Domäne, mit der Sie Ihre Tests durchführen wollen, in der lokalen Exchange-Umgebung als akzeptierte Domäne. Es muss sich dabei um dieselbe Domäne handeln, die Sie in Ihrem Microsoft 365-Testkonto verifiziert haben. Wechseln Sie dazu im EAC der lokalen Exchange-Umgebung zum Bereich NACHRICHTENFLUSS und dann zum Abschnitt AKZEPTIERTE DOMÄNEN (siehe Abbildung 6.134).

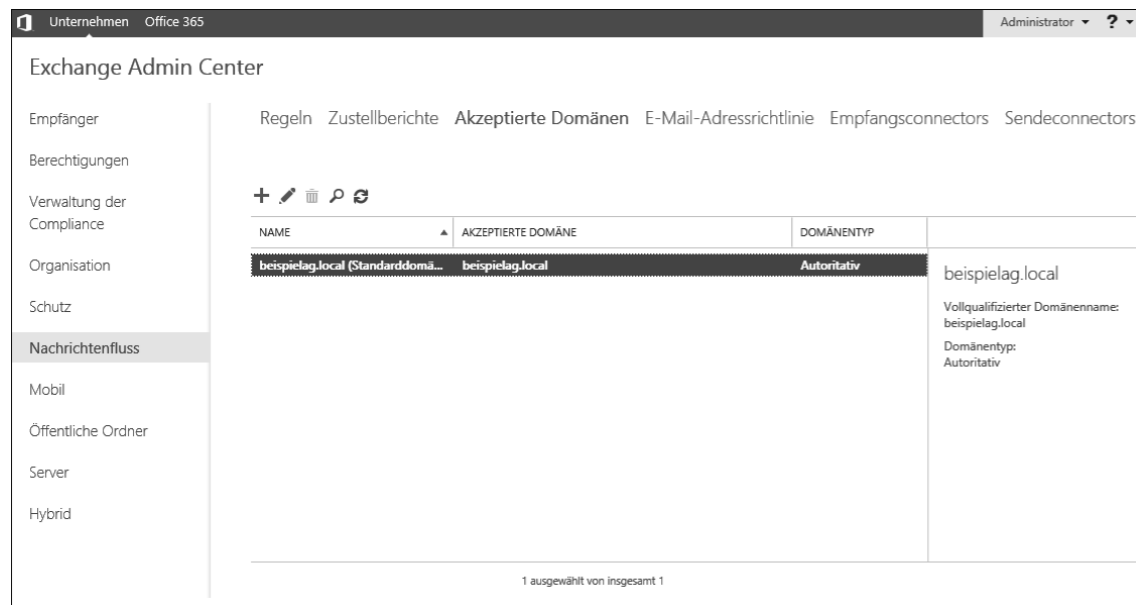


Abbildung 6.134 Akzeptierte Domänen

Nachdem Sie die Domäne hinterlegt haben, öffnen Sie den Eintrag und wählen die Option DIESE DOMÄNE ALS STANDARDDOMÄNE VERWENDEN.

Sendeconnector

Für E-Mails, die an fremde Adressen gesandt werden sollen, legen Sie einen Sendconnector an. Wechseln Sie dazu im EAC der lokalen Exchange-Umgebung zum Bereich NACHRICHTENFLUSS und dann zum Abschnitt SENDECONNECTORS (der Bezeichner wird tatsächlich so verwendet; siehe Abbildung 6.135).

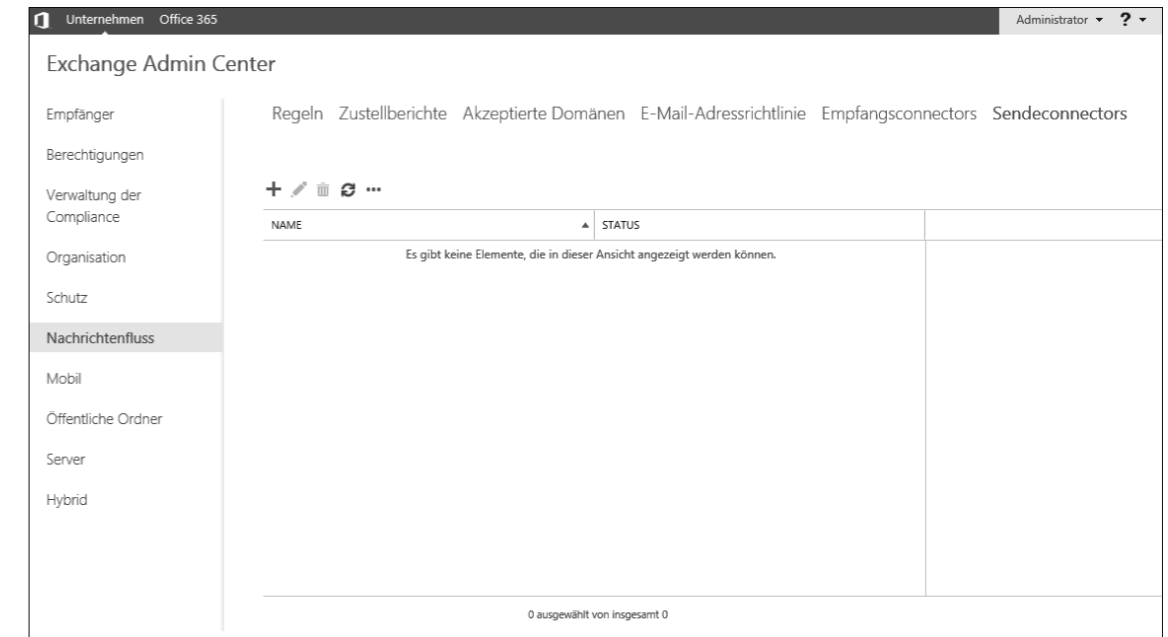


Abbildung 6.135 Sendconnectors

Beim Anlegen des neuen Sendconnectors machen Sie in Ihrer Testumgebung folgende Angaben:

- ▶ **NAME:** beliebig
- ▶ **TYP:** INTERNET
- ▶ **NETZWERKEINSTELLUNGEN:** Hier steht zur Auswahl, dass E-Mails direkt an den zuständigen Server der Empfängerdomäne ausgeliefert werden. Das setzt aber voraus, dass der empfangende Server dem anderen vertraut. Sollten daran Zweifel bestehen (beispielsweise weil Sie Ihr Testsystem hinter einem Einwahl-DSL-Zugang aufgebaut haben), nutzen Sie die Option SMARTHOST. Dabei geben Sie einen SMTP-Server (typischerweise den Ihres Providers) an, über den die E-Mails versandt werden sollen.
- ▶ **ADRESSRAUM:** *
- ▶ **QUELLSERVER:** Ihr Exchange-Testserver

E-Mail-Adressrichtlinie

Überprüfen bzw. setzen Sie die E-Mail-Adressrichtlinie, um den Postfächern eine E-Mail-Adresse für Ihre in Microsoft 365 verifizierte Domäne zuzuweisen. Sie finden die Konfiguration im EAC im Bereich NACHRICHTENFLUSS unter E-MAIL-ADRESSRICHTLINIE. Als primäre SMTP-Adresse sollte die verifizierte Domäne angegeben sein.

Vergessen Sie nach einer Änderung nicht, die Richtlinie zu markieren und auf ANWENDEN ZU klicken.

SSL-Zertifikat

Damit Sie die Hybridkonfiguration funktionsfähig einrichten können, benötigen Sie ein SSL-Zertifikat einer öffentlichen Zertifizierungsstelle. Dieses Zertifikat darf nicht selbst signiert sein. Auf einer Testumgebung, die aus genau einem Exchange Server besteht, könnten Sie das wie folgt durchführen:

1. Wechseln Sie im EAC der lokalen Exchange-Umgebung zum Bereich SERVER und dann zum Abschnitt ZERTIFIKATE (siehe Abbildung 6.136).

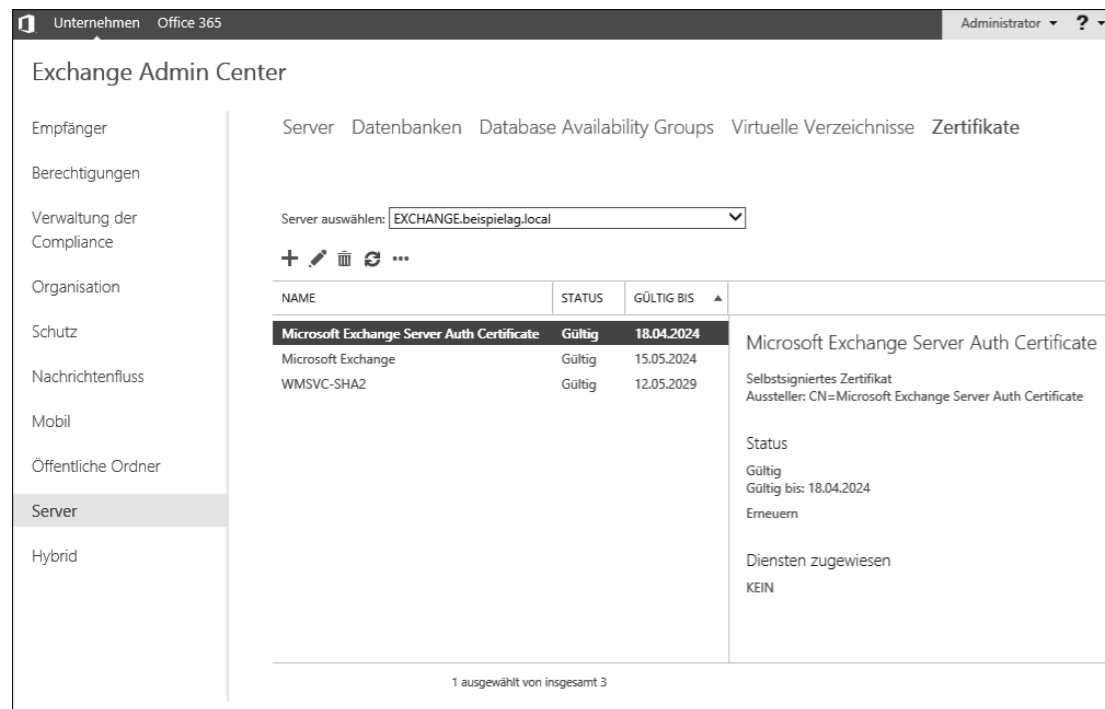


Abbildung 6.136 Zertifikatsverwaltung

2. Klicken Sie auf die Schaltfläche NEU (Plus-Symbol). Es startet ein Assistent.

3. Wählen Sie die Option ANFORDERUNG EINES ZERTIFIKATS VON EINER ZERTIFIZIERUNGSSTELLE ERSTELLEN.
4. Geben Sie einen beliebigen Anzeigenamen für das Zertifikat an.
5. Fordern Sie gegebenenfalls ein Platzhalterzertifikat an.
6. Geben Sie den oder die Server an, auf dem bzw. denen das Zertifikat gespeichert werden soll.
7. Wählen Sie die Domänen aus, die im Zertifikat enthalten sein sollen.
8. Geben Sie Name, Abteilung, Land, Ort und Bundesland an.
9. Geben Sie einen Pfad zu einer REQ-Datei ein, mit deren Hilfe Sie bei einer öffentlichen Zertifizierungsstelle ein passendes Zertifikat anfordern können.

Mit der REQ-Datei lassen Sie sich nun bei einer öffentlichen Zertifizierungsstelle ein passendes Zertifikat ausstellen. Dieses Zertifikat müssen Sie dann in Ihre Exchange-Organisation importieren:

1. Wechseln Sie im EAC der lokalen Exchange-Umgebung zum Bereich SERVER und dann zum Abschnitt ZERTIFIKATE.
2. Markieren Sie in der angezeigten Liste die Zertifikatsanfrage, und wählen Sie den Befehl ABSCHLIESSEN.
3. Geben Sie die von der Zertifizierungsstelle erhaltene Antwortdatei an.
4. Markieren Sie in der Liste das Zertifikat, und klicken Sie auf BEARBEITEN (Stift-Symbol).
5. Wechseln Sie zum Bereich DIENSTE, und markieren Sie die Dienste SMTP und IIS (siehe Abbildung 6.137).

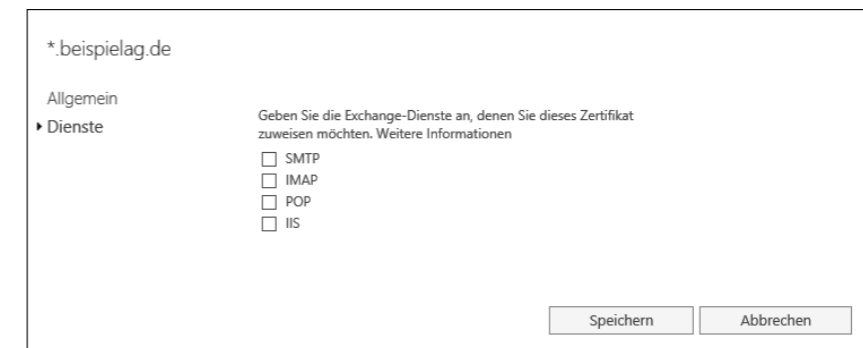


Abbildung 6.137 Dienste auswählen

Anpassung externer URLs

Nachdem das Zertifikat eingerichtet wurde, überprüfen bzw. setzen Sie noch die externen URLs für ECP (EAC), OWA, Offlineadressbuch (OAB) und für die Exchange-Webdienste. Mit

den folgenden Befehlen überprüfen Sie die aktuellen Einstellungen (wurde diese Konfiguration noch nie gemacht, ist die Ausgabe jeweils leer):

```
Get-EcpVirtualDirectory |
  Select-Object InternalUrl,ExternalUrl
Get-OwaVirtualDirectory |
  Select-Object InternalUrl,ExternalUrl
Get-OabVirtualDirectory |
  Select-Object InternalUrl,ExternalUrl
Get-WebServicesVirtualDirectory |
  Select-Object InternalUrl,ExternalUrl
```

#Bei Exchange 2019/2016:

```
Get-MapiVirtualDirectory |
  Select-Object InternalUrl,ExternalUrl
```

Listing 6.55 Externe URLs ermitteln

Bei einer simplen Testinstallation sollte es bei jedem Get-Cmdlet nur jeweils eine Rückgabe geben. Sie können externe URLs dann wie folgt setzen:

```
Get-EcpVirtualDirectory |
  Set-EcpVirtualDirectory -ExternalUrl <url>
Get-OwaVirtualDirectory |
  Set-OwaVirtualDirectory -ExternalUrl <url>
Get-OabVirtualDirectory |
  Set-OabVirtualDirectory -ExternalUrl <url>
Get-WebServicesVirtualDirectory |
  Set-WebServicesVirtualDirectory -ExternalUrl <url>
```

#Bei Exchange 2019/2016

```
Get-MapiVirtualDirectory |
  Set-MapiVirtualDirectory -ExternalUrl <url>
```

Listing 6.56 Externe URLs setzen

In Abbildung 6.138 sehen Sie ein Beispiel.

Outlook Anywhere-Domäne

Nun muss noch der externe *Hostname* für *Outlook Anywhere* konfiguriert werden.



Outlook Anywhere erlaubt eine gesicherte Verbindung aus dem Internet mit der Exchange-Umgebung ohne den Einsatz eines VPNs.

```
Computer: EXCHANGE.beispielag.local
[PS] C:\>Get-EcpVirtualDirectory | Select-Object InternalUrl,ExternalUrl
InternalUrl          ExternalUrl
-----
https://exchange.beispielag.local/ecp https://exchange.beispielag.de/ecp

[PS] C:\>Get-OwaVirtualDirectory | Select-Object InternalUrl,ExternalUrl
InternalUrl          ExternalUrl
-----
https://exchange.beispielag.local/owa https://exchange.beispielag.de/owa

[PS] C:\>Get-OabVirtualDirectory | Select-Object InternalUrl,ExternalUrl
InternalUrl          ExternalUrl
-----
https://exchange.beispielag.local/OAB https://exchange.beispielag.de/OAB

[PS] C:\>Get-WebServicesVirtualDirectory | Select-Object InternalUrl,ExternalUrl
InternalUrl          ExternalUrl
-----
https://exchange.beispielag.local/EWS/Exchange.asmx https://exchange.beispielag.de/EWS/Exchange.asmx

[PS] C:\>Get-MapiVirtualDirectory | Select-Object InternalUrl,ExternalUrl
InternalUrl          ExternalUrl
-----
https://exchange.beispielag.local/mapi https://exchange.beispielag.de/mapi

[PS] C:\>
```

Abbildung 6.138 Externe URL für ECP einrichten

Starten Sie dazu auf Ihrem lokalen Exchange Server die EMS. Um die aktuelle Einstellung zu überprüfen, geben Sie folgendes Kommando:

```
Get-OutlookAnywhere | Format-List ExternalHostname
```

Listing 6.57 Externen Hostnamen abfragen

Setzen Sie dann den externen Hostnamen auf den Domänennamen, unter dem Ihr Exchange Server aus dem Internet erreichbar ist:

```
Get-OutlookAnywhere |
  Set-OutlookAnywhere -ExternalHostname <DOMÄNE> `
  -ExternalClientsRequireSsl $true `
  -ExternalClientAuthenticationMethod Negotiate
```

Listing 6.58 Externen Hostnamen setzen

Verbindungstests

Wie schon mehrfach angesprochen wurde, können Sie die korrekte Funktionsweise der Schnittstellen Ihres lokalen Exchange Servers über den Remote Connectivity Analyzer überprüfen:

<https://testconnectivity.microsoft.com>

Für eine Exchange-Hybridumgebung sollten dabei die folgenden Tests ohne Fehler durchlaufen werden (alle auf der Registerkarte EXCHANGE SERVER):

- ▶ OUTLOOK-AUTOERMITTLUNG
- ▶ OUTLOOK-VERBINDUNG
- ▶ SYNCHRONISIERUNG, BENACHRICHTIGUNG, VERFÜGBARKEIT UND AUTOMATISCHE ANTWORTEN



Sollten Sie beim Ausführen der Tests Probleme bei der gegenseitigen Authentifizierung erhalten, hilft Ihnen folgender Artikel weiter:

[https://docs.microsoft.com/de-de/previous-versions/office/exchange-remote-connectivity/dd439371\(v=exchg.80\)](https://docs.microsoft.com/de-de/previous-versions/office/exchange-remote-connectivity/dd439371(v=exchg.80))

Den Postfachreplikationsdienst einrichten

Das Verschieben der Postfächer zu Exchange Online übernimmt der *Postfachreplikationsdienst* (MRS für *Mailbox Replication Service*). Dieser muss gegebenenfalls zunächst aktiviert werden.

Starten Sie die Exchange Management Shell (EMS) auf einem lokalen Exchange Server, und führen Sie folgendes Kommando aus:

```
Get-WebServicesVirtualDirectory |
  Select-Object Name, MRSProxyEnabled
```

Listing 6.59 Abfrage des Postfachreplikationsdienstes

Sollte in der Spalte `MRSProxyEnabled` der Wert `False` stehen, können Sie den Postfachreplikationsdienst über folgendes Kommando aktivieren:

```
Set-WebServicesVirtualDirectory `
  -Identity "EWS (Default Web Site)" `
  -MRSProxyEnabled $True
```

Listing 6.60 Postfachreplikationsdienst aktivieren

Danach ist gegebenenfalls ein Neustart des Servers erforderlich.

6.10.5 Einrichtung

Die Hybridkonfiguration richten Sie mithilfe eines Assistenten über das EAC des Exchange Servers ein. Wie ich bereits angesprochen habe, sollten Sie darauf achten, vorab alle vorhandenen Service Packs und Cumulative Updates einzuspielen.

In diesem Abschnitt verwende ich einen Exchange Server 2019. Mit den Versionen 2013 und 2016 sind die Schritte jedoch grundsätzlich identisch.



Der Assistent nimmt während der Einrichtung folgende Konfigurationen vor:

- ▶ Er erzeugt im lokalen Active Directory das Objekt *HybridConfiguration*. Dieses Objekt ist für die Konfigurationsdaten der Hybridkonfiguration vorgesehen und wird vom Assistenten mit Ihren Angaben gefüllt. Während dieser Einrichtung der Hybridkonfiguration wird die Konfiguration auf Basis dieses Objekts vorgenommen.
 - Jedes Mal, wenn Sie den Assistenten starten, wird das Objekt zurückgesetzt und mit den neuen Angaben überschrieben.
- ▶ Der Assistent erstellt eine Verbundvertrauensstellung mit dem *Microsoft Federation Gateway* und ein selbst signiertes Zertifikat für die Absicherung der Kommunikation.
- ▶ Er überprüft, ob alle Berechtigungen und Voraussetzungen erfüllt sind.
- ▶ Er nimmt die Einrichtung der Hybridkonfiguration und die Aktivierung folgender Funktionalitäten vor:
 - gemeinsame Verfügbarkeitsinformationen
 - Verschieben von Postfächern
 - gemeinsame Nachrichtenverfolgung
 - gemeinsame MailTips
 - Archivierung in Exchange Online
 - Outlook im Web-Umleitung
 - sichere Nachrichtenübertragung zwischen den Exchange-Organisationen (TLS)

Sehen wir uns die Konfiguration mithilfe des Assistenten einmal genauer an:

1. Öffnen Sie auf einem Windows Server, der sich in derselben Domäne wie der lokale Exchange Server befindet, den Hybrid-Konfigurationsassistenten unter der folgenden URL:

<https://aka.ms/hybridwizard>

 Damit wird der Hybridkonfigurations-Assistent heruntergeladen und gestartet (siehe Abbildung 6.139). Sollte es bei der Konfiguration zu einem Fehler kommen, können Sie den Assistenten später erneut starten. Dazu finden Sie nach dem ersten Start auf dem Desktop ein Anwendungssymbol.
2. Im Schritt `LOKALE EXCHANGE SERVER-ORGANISATION` versucht der Assistent nun automatisch, einen geeigneten Exchange Server ausfindig zu machen (siehe Abbildung 6.140).



Abbildung 6.139 Hybridkonfigurations-Assistent

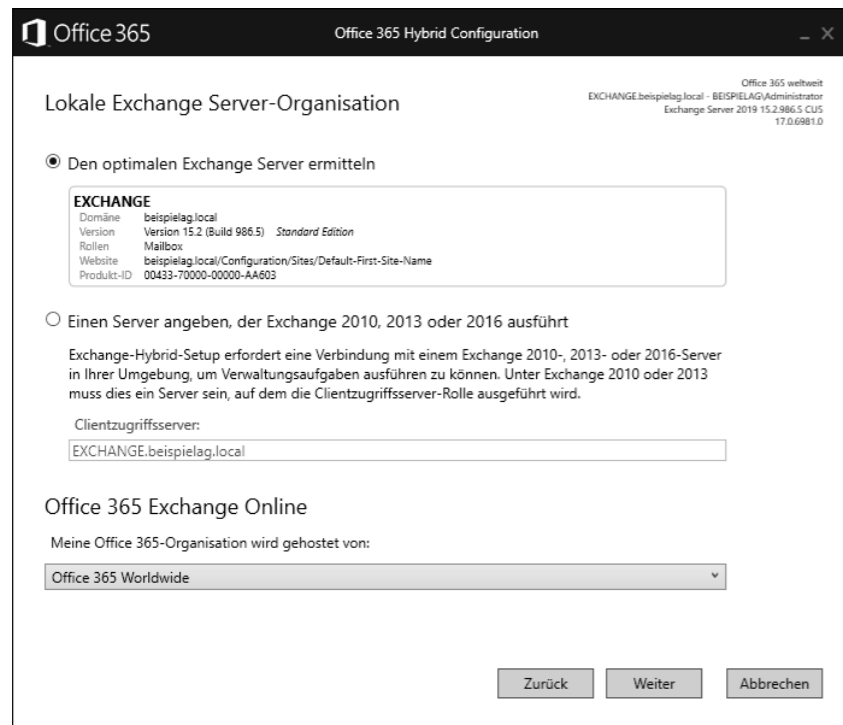


Abbildung 6.140 Lokale Exchange Server-Organisation

Sollte das nicht erfolgreich sein, geben Sie selbst einen Clientzugriffs-Server mit Exchange 2010, 2013, 2016 oder 2019 an. Außerdem geben Sie an, wo Ihr Mandant angelegt ist (im Normalfall OFFICE 365 WORLDWIDE).

3. Im Schritt ANMELDEINFORMATIONEN geben Sie die Benutzerdaten eines lokalen Exchange- und eines Microsoft 365-Administrators an (siehe Abbildung 6.141).

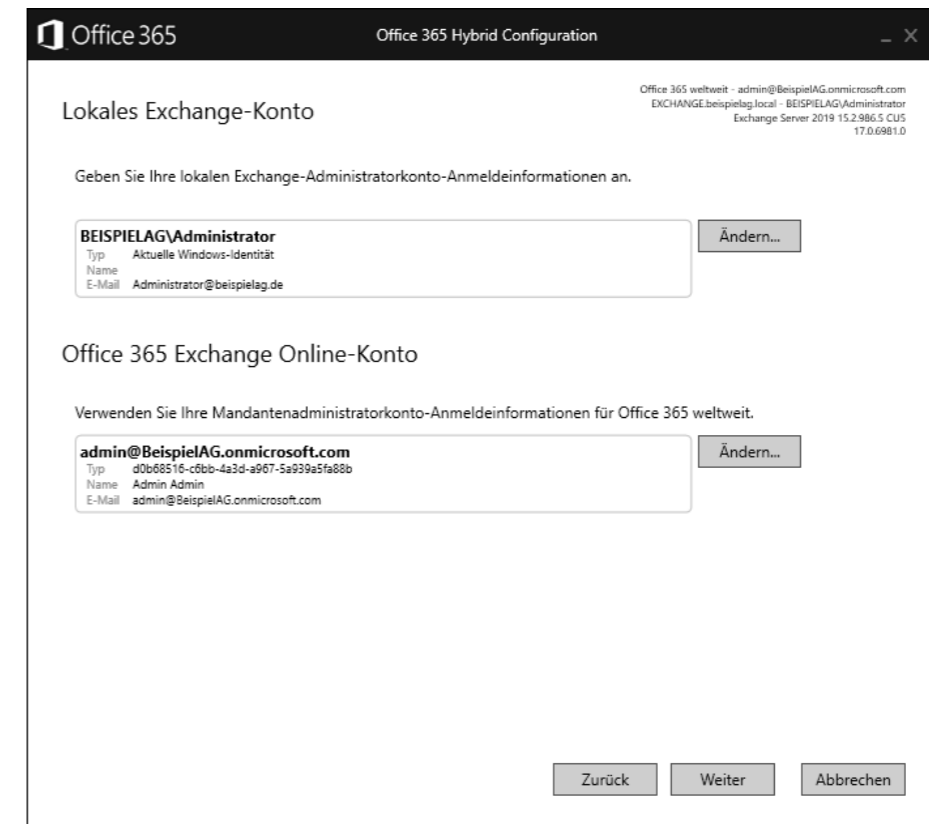


Abbildung 6.141 Anmeldeinformationen

4. Im Schritt HYBRIDFUNKTIONEN entscheiden Sie sich wahlweise für die MINIMALE HYBRIDKONFIGURATION oder die VOLLSTÄNDIGE HYBRIDKONFIGURATION (siehe Abbildung 6.142). Hier in diesem Abschnitt machen wir mit der VOLLSTÄNDIGEN HYBRIDKONFIGURATION weiter.
5. Im Schritt HYBRIDTOPOLOGIE wählen Sie die gewünschte Exchange-Konfiguration aus (siehe Abbildung 6.143). Im Beispiel verwende ich die KLASSISCHE EXCHANGE-HYBRIDTOPOLOGIE.



Abbildung 6.142 Hybridfunktionen

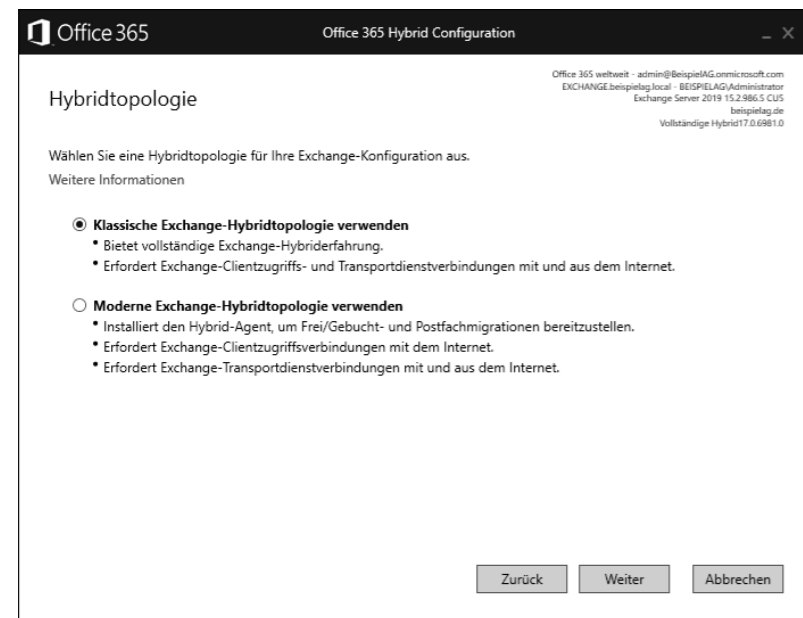


Abbildung 6.143 Hybridtopologie

6. Im Schritt **LOKALES KONTO FÜR MIGRATION** geben Sie die Anmeldeinformationen für die lokale Exchange-Umgebung an, über die ein Migrationsendpunkt erzeugt wird (siehe Abbildung 6.144).

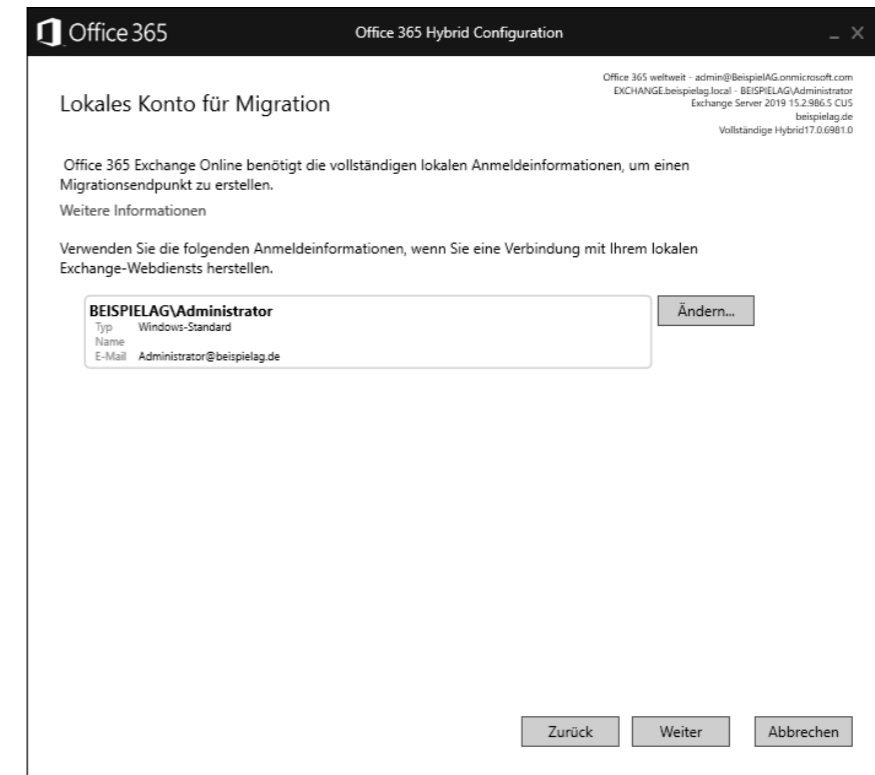


Abbildung 6.144 Lokales Konto für Migration

7. Entscheiden Sie sich im Schritt **HYBRIDKONFIGURATION** für einen Transportpfad (siehe Abbildung 6.145). Zur Auswahl stehen die standardmäßig verwendete Konfiguration des Clientzugriffs- und Postfachservers und alternativ die Konfiguration eines Edge-Transport-Servers.

Unter **ERWEITERT** können Sie außerdem den zentralen E-Mail-Transport aktivieren (siehe Abschnitt 6.10.1, »E-Mail-Verkehr«).

In diesem Beispiel verwenden wir die Standardvorgehensweise über Clientzugriffs- und Postfachserver.

8. Im Schritt **EMPFANGSCONNECTORKONFIGURATION** wählen Sie mindestens einen lokalen Clientzugriffs-Server für die Empfangsrichtung aus (siehe Abbildung 6.146).



Abbildung 6.145 Hybridkonfiguration

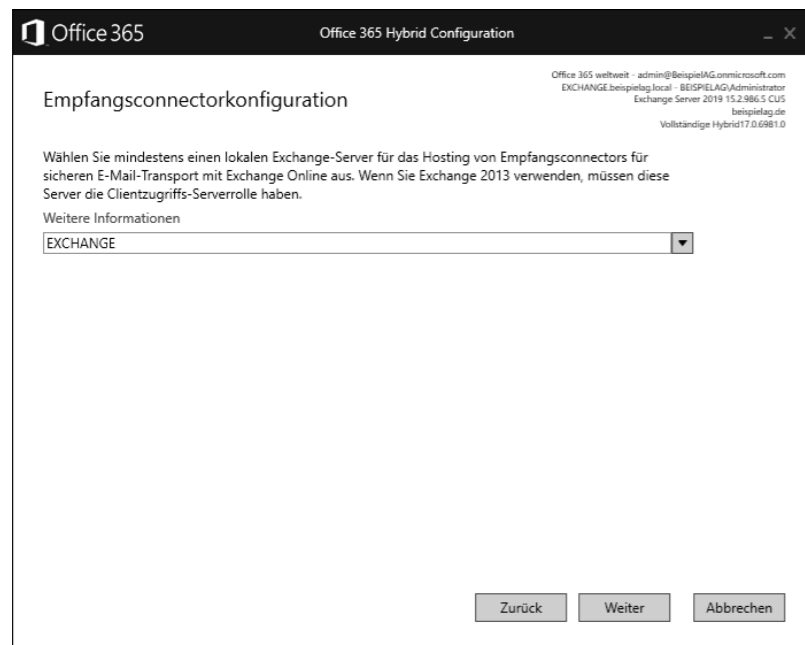


Abbildung 6.146 Empfangsconnectorkonfiguration

9. Im Schritt SENDECONNECTORKONFIGURATION wählen Sie mindestens einen Postfachserver für die Senderichtung aus (siehe Abbildung 6.147).



Abbildung 6.147 Sendecollectorkonfiguration

10. Im Schritt TRANSPORTZERTIFIKAT wählen Sie das Zertifikat aus, mit dem der Nachrichtenfluss abgesichert werden soll (siehe Abbildung 6.148).
11. Im Schritt ORGANISATIONS-FQDN geben Sie einen (externen) FQDN (*Full Qualified Domain Name* oder auf Deutsch *vollqualifizierter Domänenname*) eines Ihrer Postfachserver ein, der von Exchange Online zur Weiterleitung von Nachrichten genutzt werden soll (siehe Abbildung 6.149).
12. Klicken Sie nun auf die Schaltfläche AKTUALISIEREN, beginnt der Hybrid-Assistent mit der Konfiguration.

Wenn alles geklappt hat, können Sie versuchen, ein lokales Postfach zu Exchange Online zu verschieben, ein lokales Postfach mit einem Archivpostfach in Exchange Online auszustatten etc.

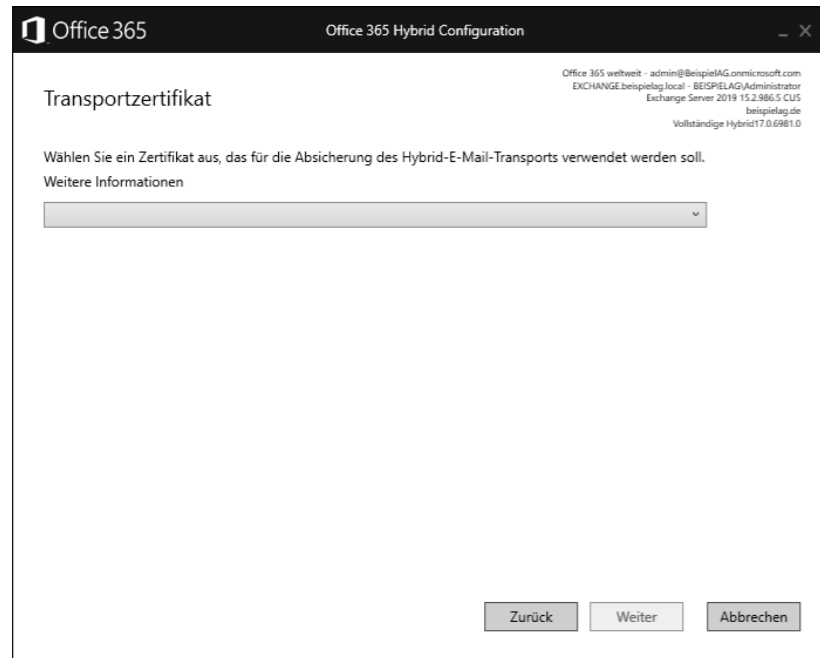


Abbildung 6.148 Transportzertifikat

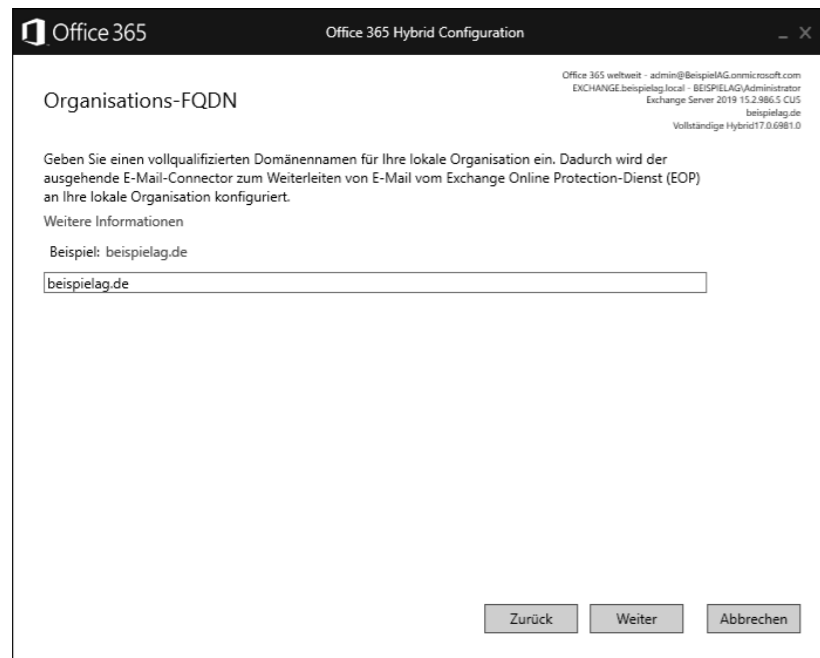


Abbildung 6.149 Organisations-FQDN

Außerdem sollten Sie testweise E-Mails verschicken, und zwar in folgenden Konstellationen:

- ▶ von einem lokalen Postfach an ein lokales Postfach
- ▶ von einem Online-Postfach an ein Online-Postfach
- ▶ von einem lokalen Postfach an ein Online-Postfach
- ▶ von einem Online-Postfach an ein lokales Postfach
- ▶ von einem externen Postfach an ein lokales Postfach
- ▶ von einem externen Postfach an ein Online-Postfach

6.10.6 Postfächer verschieben

In einer Hybridkonfiguration haben Sie die Möglichkeit, in der lokalen Exchange-Organisation vorhandene Postfächer zu Exchange Online zu verschieben (*Onboarding*). Aber auch die andere Richtung ist denkbar: Ein Postfach aus Exchange Online wird zur lokalen Exchange-Organisation verschoben (*Offboarding*).

Sollte es bei der Verschiebung zu unerwarteten Problemen kommen, hilft vielleicht der von Microsoft bereitgestellte *Hybrid Migration Troubleshooter* weiter. Er hilft bei der Problemlösung und ist über folgende URL erreichbar:

<https://docs.microsoft.com/en-US/exchange/troubleshoot/move-or-migrate-mailboxes/troubleshoot-migration-issues-in-exchange-hybrid>

Nachdem Sie Postfächer zwischen den Organisationen verschoben haben, sollten Sie die Berechtigungen daraufhin überprüfen, ob sie noch so gesetzt sind, wie Sie es wünschen. *Senden im Auftrag*-Berechtigungen werden nur berücksichtigt, wenn beide beteiligten Postfächer gemeinsam verschoben werden. *Senden als*- und *Vollzugriffsberechtigungen* gehen verloren.

In die Cloud ...

Nehmen wir an, Sie haben einen Benutzer samt Postfach in der lokalen Exchange-Organisation. Dieses Postfach soll zu Exchange Online verschoben werden. Gehen Sie wie folgt vor:

1. Im EAC von Exchange Online wechseln Sie zum Bereich EMPFÄNGER und dort zum Abschnitt MIGRATION (siehe Abbildung 6.150).
2. Klicken Sie auf MIGRATIONSBATCHE HINZUFÜGEN, erscheint der E-Mail-Migrations-Assistent (siehe Abbildung 6.151).
3. Geben Sie einen Namen für den Migrationsbatch ein, und wählen Sie als POSTFACH-MIGRATIONSPFAD die Option MIGRATION ZU EXCHANGE ONLINE.

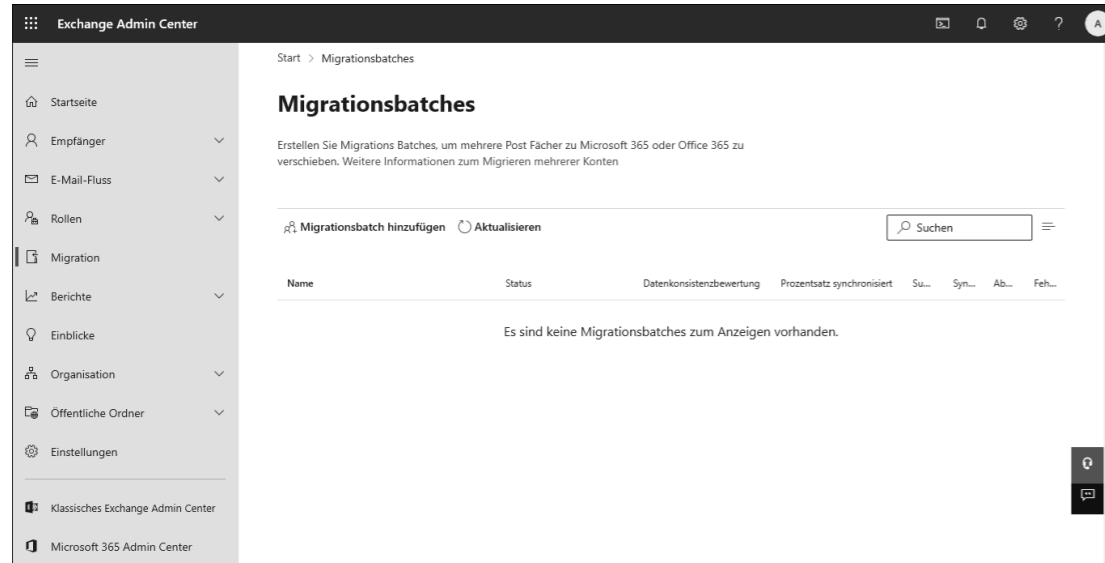


Abbildung 6.150 Migrations-Bereich im EAC

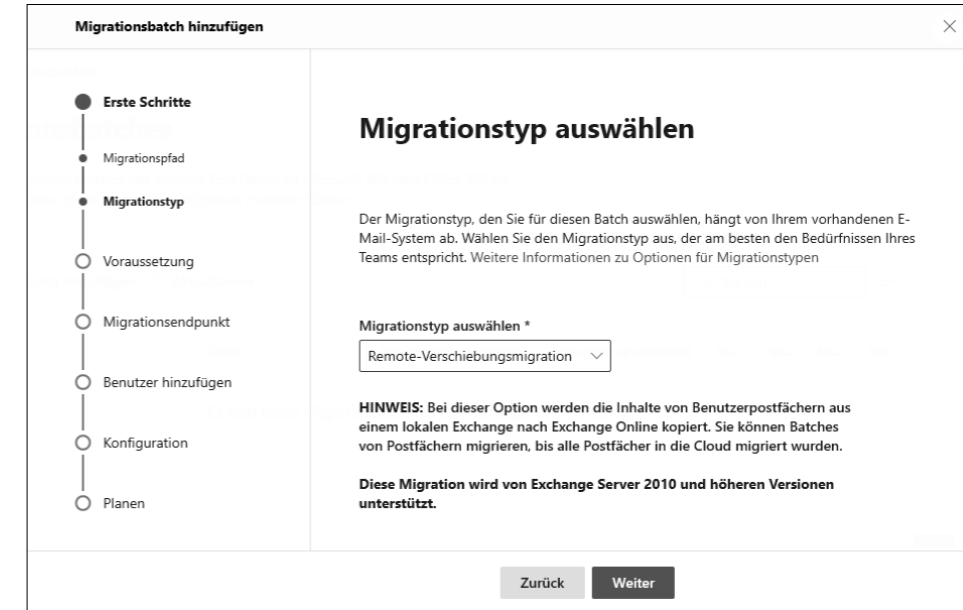


Abbildung 6.152 Migrationstyp

5. Lesen und beachten Sie im Schritt VORAUSSETZUNG die Hinweise (siehe Abbildung 6.153).

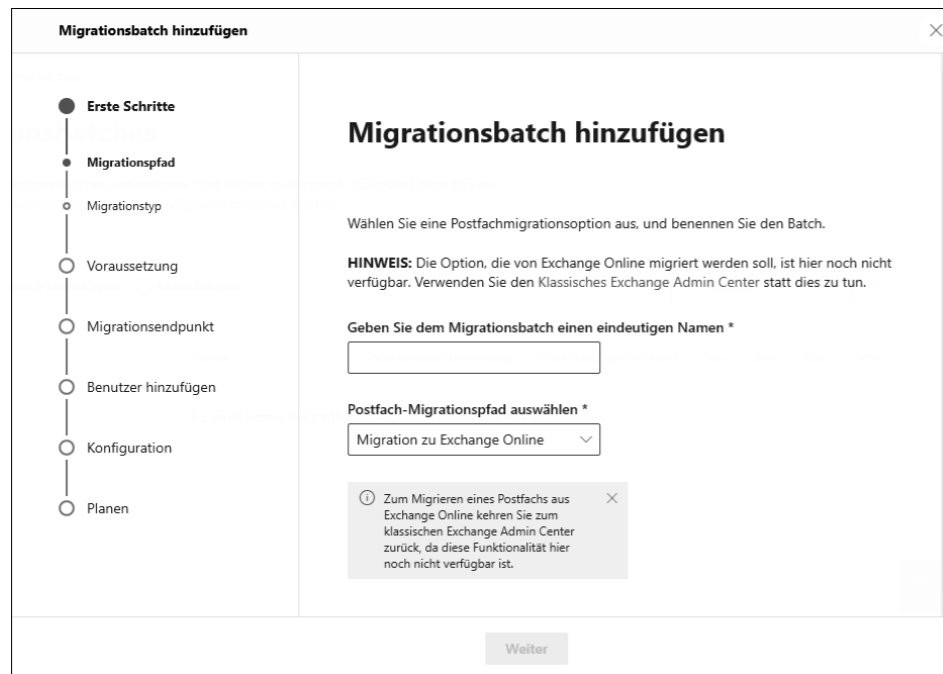


Abbildung 6.151 Der E-Mail-Migrations-Assistent

4. Im Schritt MIGRATIONSTYP wählen Sie die Option REMOTE-VERSCHIEBUNGSMIGRATION (siehe Abbildung 6.152).

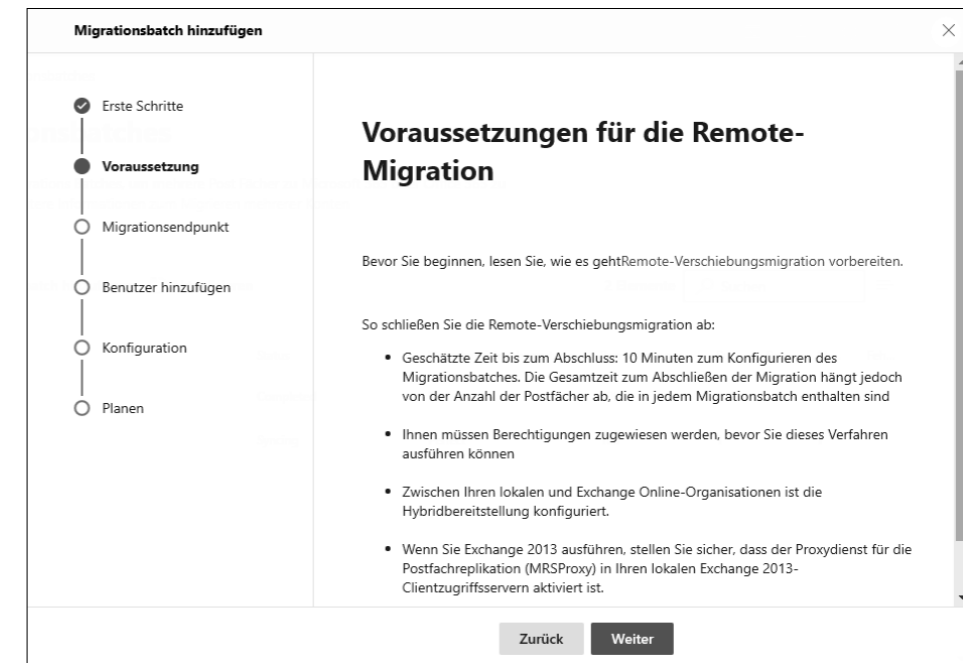


Abbildung 6.153 Voraussetzungen

6. Im Schritt **MIGRATIONSENDPUNKT** wählen Sie eben diesen aus (siehe Abbildung 6.154). Der Migrationsendpunkt wurde bei der Einrichtung vom Hybrid-Konfigurationsassistenten erstellt.

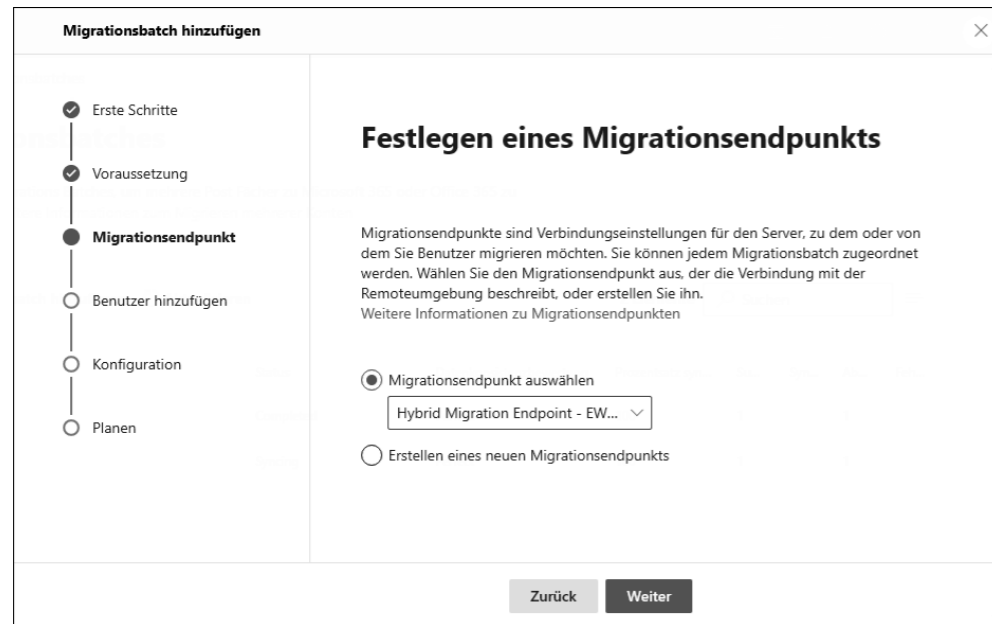


Abbildung 6.154 Migrationsendpunkt

7. Wählen Sie im Schritt **BENUTZER HINZUFÜGEN** die zu verschiebenden Benutzer aus, oder laden Sie eine CSV-Datei mit den E-Mail-Adressen der zu verschiebenden Benutzer hoch (siehe Abbildung 6.155).

Die CSV-Datei legen Sie mit der Spalte `EmailAddress` an und hinterlegen in jeder Zeile eine E-Mail-Adresse.

Sollte in der Benutzerauswahlliste ein Benutzer mit lokalem Postfach nicht enthalten sein, liegt das möglicherweise daran, dass für den Benutzer bereits ein Exchange Online-Postfach existiert. Damit ist das Verschieben des lokalen Postfachs nicht möglich. Diese Situation kann auftreten, wenn Sie vor der Aktivierung der Exchange-Hybridkonfiguration im Verzeichnissynchronisierungstool dem Benutzer eine Exchange Online-Lizenz zugewiesen haben. Damit wird automatisch ein Exchange Online-Postfach angelegt. Das geschieht aber nicht, wenn im Verzeichnissynchronisierungstool die Hybridkonfiguration aktiviert ist und der Benutzer bereits über ein lokales Postfach verfügt.

8. Im Schritt **KONFIGURATION** geben Sie die **ZIELZUSTELLUNGSDOMÄNE** an (siehe Abbildung 6.156). Achtung: Geben Sie hier nicht (!) Ihre eigene Domäne an, sondern die Domäne mit der Endung `mail.onmicrosoft.com`.

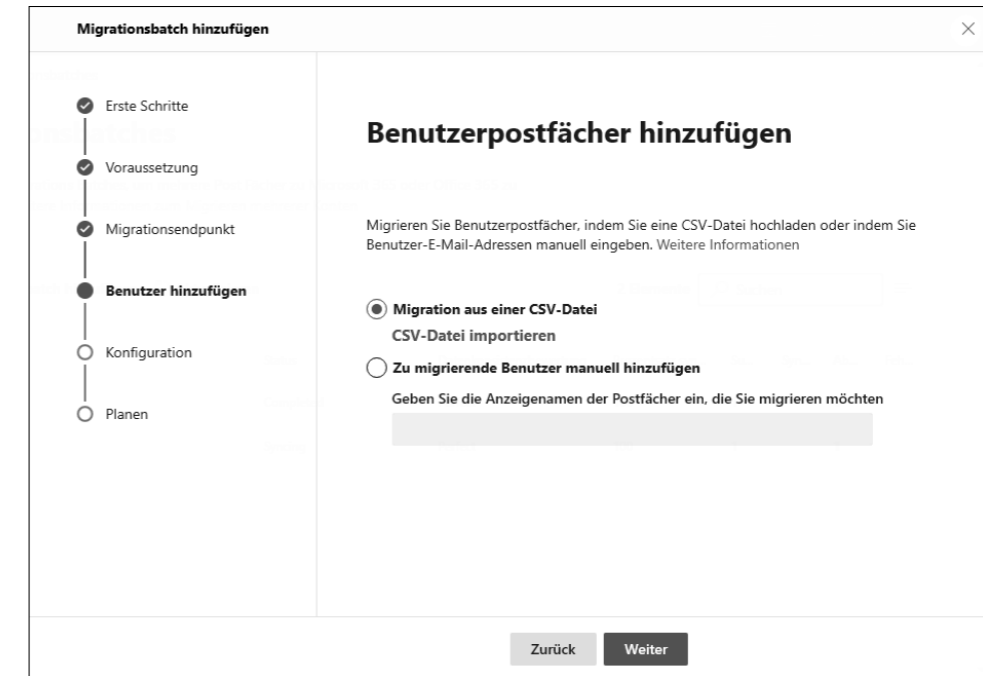


Abbildung 6.155 Benutzer hinzufügen

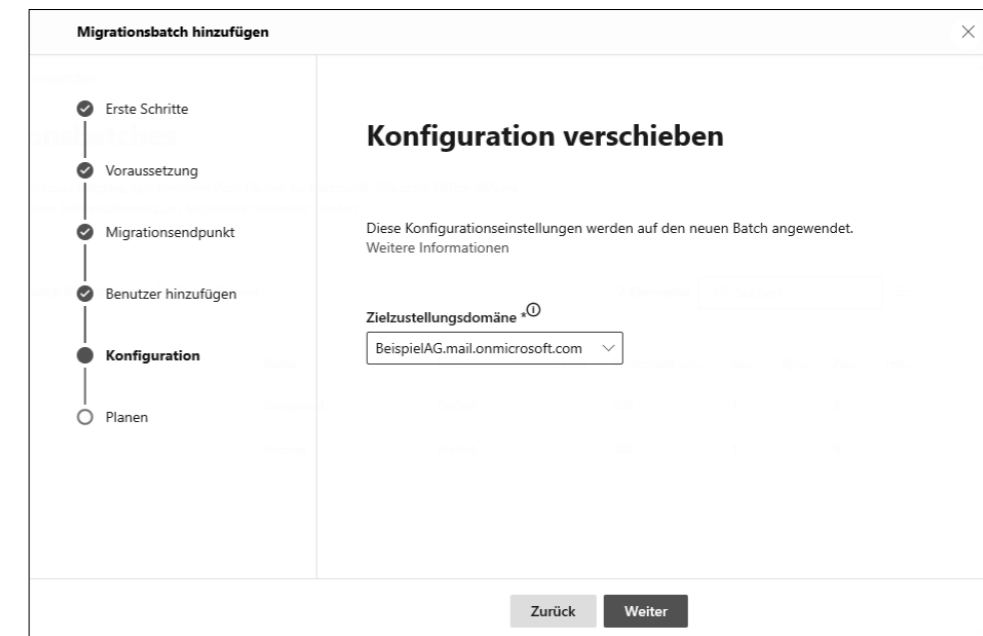


Abbildung 6.156 Konfiguration

9. Im letzten Schritt, PLANEN, geben Sie einen Microsoft 365-Benutzer an, der über den Fortschritt der Migration per E-Mail benachrichtigt wird (siehe Abbildung 6.157). Außerdem entscheiden Sie, ob die Migration unmittelbar oder zu einem späteren Zeitpunkt begonnen werden soll. Die Option MIGRATIONS BATCH AUTOMATISCH ABSCHLIESSEN wählen Sie, um dies nicht selbst nach dem Verschiebevorgang tun zu müssen.

Migrationsbatch hinzufügen

Batchmigration planen

Ein neuer Migrationsbatch wird erstellt, nachdem Sie auf "Speichern" geklickt haben. Der Batch wird innerhalb weniger Stunden in die Warteschlange gestellt und verarbeitet. Weitere Informationen

Nach Abschluss des Batches wird ein Bericht an die folgenden Empfänger gesendet. Sie müssen mindestens einen Empfänger auswählen, der diesen Bericht erhalten soll. *

Admin × Namen oder E-Mail-Adresse suchen

Migrationsbatch starten bis *

Batch zu einem späteren Zeitpunkt manuell starten (durch Auswählen des Batches im Migrationsdashboard und anschließendes Klicken auf „Start“)

Batch automatisch starten

Batch nach folgender Zeit automatisch starten: -

Zurück Speichern

Abbildung 6.157 Planen

10. Damit schließen Sie den Assistenten. Das EAC zeigt den neuen Migrationsbatch an (siehe Abbildung 6.158).
11. Falls Sie sich für einen späteren Start der Migration entschieden haben, markieren Sie den Migrationsbatch und klicken dann auf die Schaltfläche MIGRATION STARTEN, um mit der Migration zu beginnen.

Verwendet der Anwender Outlook, kann er während des Verschiebens weiterhin mit seinem Postfach arbeiten. Nachdem das Postfach verschoben wurde, erhält er den Hinweis, er möge Outlook neu starten. Die bereits bestehende OST-Datei bleibt dabei erhalten.



Vergessen Sie nicht, dem Benutzer in Microsoft 365 gegebenenfalls noch eine Exchange Online-Lizenz zuzuweisen und – sofern Sie keinen Domänenverbund für Single Sign-on oder die Pass-Through-Authentication konfiguriert haben – auch ein Kennwort.

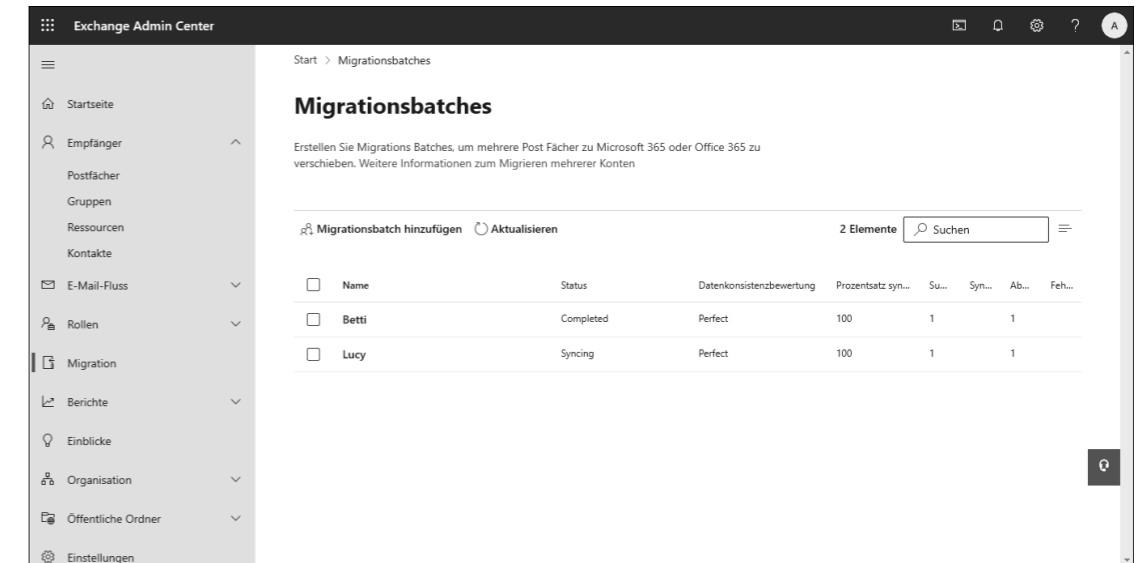


Abbildung 6.158 Migrationsfortschritt

Das Verschieben von Postfächern können Sie natürlich auch im großen Stil mit der PowerShell von Exchange Online aus erledigen. Hier ein Beispiel:

```
#Datei mit zu verschiebenden Postfach-E-Mail-Adressen
$datei = "Benutzer.csv"

#Zielzustellungsdomäne
$domaene = "beispielag.de"

#Endpunkt abfragen
$endpunkt = Get-MigrationEndpoint -Identity "Endpunkt"

#Batch anlegen und starten
New-MigrationBatch -Name "Batch" `
  -SourceEndpoint $endpunkt.Identity `
  -TargetDeliveryDomain $domaene `
  -CSVData ([System.IO.File]::ReadAllBytes($datei)) `
  -AutoStart `
  -AutoComplete
```

Listing 6.61 Postfach zu Exchange Online verschieben

Im Beispiel wird der Verschiebevorgang automatisch gestartet (durch den Parameter -AutoStart) und abgeschlossen (Parameter -AutoComplete). Soll nur das Archivpostfach verschoben werden, geben Sie zusätzlich noch den Parameter -ArchiveOnly an.

... und wieder zurück

Der umgekehrte Weg, ein Postfach aus Exchange Online in die lokale Exchange-Organisation zu verschieben, hat es aktuell noch nicht in das neue EAC geschafft, sondern ist nur im klassischen EAC vorhanden. Öffnen Sie dieses über die Navigationsleiste des EAC:

1. Im Bereich EMPFÄNGER wechseln Sie zum Abschnitt MIGRATION.
2. Klicken Sie auf NEU (Plus-Symbol), und wählen Sie den Befehl VON EXCHANGE ONLINE MIGRIEREN. Dann erscheint der E-Mail-Migrations-Assistent.
3. Wählen Sie entweder die zu verschiebenden Benutzer aus, oder laden Sie eine CSV-Datei mit den E-Mail-Adressen der zu verschiebenden Benutzer hoch. Die CSV-Datei hat den identischen Aufbau wie in der umgekehrten Verschieberichtung.
4. Bestätigen Sie den Migrationsendpunkt.
5. Geben Sie einen Namen für den Migrationsbatch an. Als ZIELZUSTELLUNGSDOMÄNE geben Sie Ihre E-Mail-Domäne an (also nicht die, die auf *mail.onmicrosoft.com* endet).
Außerdem entscheiden Sie, ob das primäre Postfach samt dem (möglicherweise vorhandenen) Archivpostfach verschoben werden soll oder nur das primäre Postfach.
Zuletzt geben Sie noch den Namen der ZIELDATENBANK und gegebenenfalls den Namen der ZIELARCHIVDATENBANK an.
6. Als Nächstes können Sie einen Microsoft 365-Benutzer auswählen, der über den Fortschritt der Migration per E-Mail benachrichtigt wird. Außerdem entscheiden Sie, ob die Migration unmittelbar oder zu einem späteren Zeitpunkt begonnen werden soll. Die Option MIGRATIONSBATCHE AUTOMATISCH ABSCHLIESSEN wählen Sie, um dies nicht selbst nach dem Verschiebevorgang tun zu müssen.
7. Ein Klick auf NEU beendet den Assistenten. Das EAC zeigt den neuen Migrationsbatch an.
8. Falls Sie sich für einen späteren Start der Migration entschieden haben, markieren Sie den Migrationsbatch und klicken auf die Schaltfläche START (Dreieck-Symbol), um mit der Migration zu beginnen.

Über die PowerShell wäre dies ein Alternativbeispiel – wieder von Exchange Online aus:

```
#Datei mit zu verschiebenden Postfach-E-Mail-Adressen
$datei = "Benutzer.csv"

#Zielzustellungsdomäne
$domaene = "beispielag.de"

#Postfachdatenbank
$datenbank = "MBXDB1"
```

```
#Endpunkt abfragen
$endpunkt = Get-MigrationEndpoint -Identity "Endpunkt"

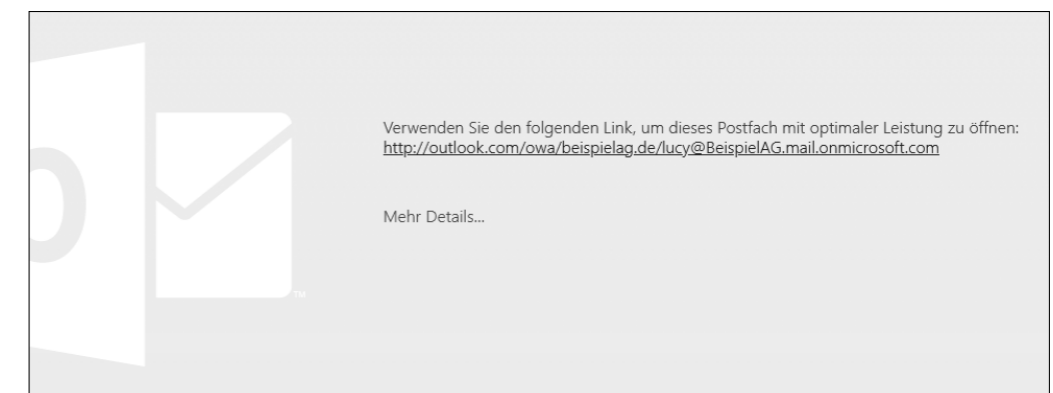
#Batch anlegen und starten
New-MigrationBatch -Name "Batch" `
  -TargetEndpoint $endpunkt.Identity `
  -TargetDeliveryDomain $domaene `
  -TargetDatabases $datenbank `
  -CSVData ([System.IO.File]::ReadAllBytes($datei)) `
  -AutoStart `
  -AutoComplete
```

Listing 6.62 Postfach von Exchange Online verschieben

Bei der Angabe der Postfachdatenbanken können Sie auch mehrere Datenbanken, durch Kommata getrennt, angeben.

6.10.7 Outlook im Web-Umleitung

Vor der Einrichtung einer Hybridkonfiguration verwenden Ihre Anwender zur Anmeldung an Outlook im Web die URL Ihrer lokalen Exchange-Organisation. Wird dann das Postfach einiger Anwender zu Exchange Online verschoben, kann dies nach wie vor so bleiben. Ihre Anwender müssen sich keine neue URL merken. Der Grund dafür ist eine automatische Umleitung, wenn ein Anwender eines Exchange Online-Postfachs sich am lokalen Outlook im Web anmeldet. In Abbildung 6.159 sehen Sie die Ansicht, die sich dem Anwender nach dem Anmelden bietet.

**Abbildung 6.159** Outlook im Web-Umleitung

Sie können den hier dargestellten Link anpassen, und zwar mithilfe des Cmdlets `Set-OrganizationRelationship`. Ein Beispiel:

```
Get-OrganizationRelationship `
-Identity "On Premises to Exchange Online Organization Relationship" |
Set-OrganizationRelationship `
-TargetOWAURL "http://outlook.com/owa/beispielag.de"
```

Listing 6.63 Ändern der Outlook im Web-Umleitungs-URL

6.10.8 Verfügbarkeitsinformationen

Wenn die Hybridkonfiguration korrekt eingerichtet werden konnte, sollte ein Anwender mit lokalem Postfach die Verfügbarkeitsinformationen auch für ein cloudbasiertes Postfach erhalten – und umgekehrt. Überprüfen Sie das beispielsweise, indem Sie über Outlook im Web je ein passendes Postfach öffnen und dann gegenseitig eine Termineinladung anlegen. Klappt alles, sollte es aussehen wie in Abbildung 6.160. In dieser Abbildung hat Lucy ihr Postfach in Exchange Online, Robin hat seines lokal. Robin erstellt eine Besprechungsanfrage und fügt Lucy hinzu. Der Terminplanungs-Assistent zeigt den bereits bestehenden Termin in Lucys Kalender an.



Abbildung 6.160 Verfügbarkeitsinformationen

Sollte es hier zu Problemen kommen, beispielsweise weil die Informationen nur von einer Seite aus ersichtlich sind, überprüfen Sie die externen URLs von ECP, OWA, vom Offline-adressbuch (OAB) und von den Exchange-Webdiensten. Lesen Sie hierzu Abschnitt 6.10.4, »Testumgebung einrichten«.

6.10.9 Exchange Online-Archive

Je ein Archivpostfach können Sie bei Bedarf für jedes primäre Postfach anlegen. Dabei sind hinsichtlich dessen, wo die beiden Postfächer liegen, mehrere Szenarien denkbar:

1. primäres Postfach und Archivpostfach lokal
2. primäres Postfach und Archivpostfach in Exchange Online
3. primäres Postfach lokal und Archivpostfach in Exchange Online

Für das dritte Szenario gibt es eine spezielle Lizenz namens *Exchange Online-Archivierung*. Lesen Sie mehr dazu in Abschnitt 6.1.2, »Lizenzüberblick«.

Im EAC können Sie beim Aktivieren eines Archivpostfachs bestimmen, ob dieses lokal oder in Exchange Online liegen soll (siehe Abbildung 6.161).



Abbildung 6.161 Anlegen eines Archivpostfachs in Exchange Online

Ein bereits lokal angelegtes Archiv können Sie bei Bedarf nach Exchange Online verschieben. Lesen Sie dazu Abschnitt 6.10.6, »Postfächer verschieben«.

6.10.10 Freigabe von Kalenderinformationen

Damit Kalenderinformationen wie etwa FREI/GEBUCHT von beiden Organisationen (Exchange lokal und Exchange Online) gemeinsam genutzt werden können, legt der Hybrid-Assistent bei der Konfiguration eine Organisationsfreigabe an. Diese finden Sie im Admin Center von Exchange Online im Bereich ORGANISATION und dort im Abschnitt TEILEN (siehe Abbildung 6.162).

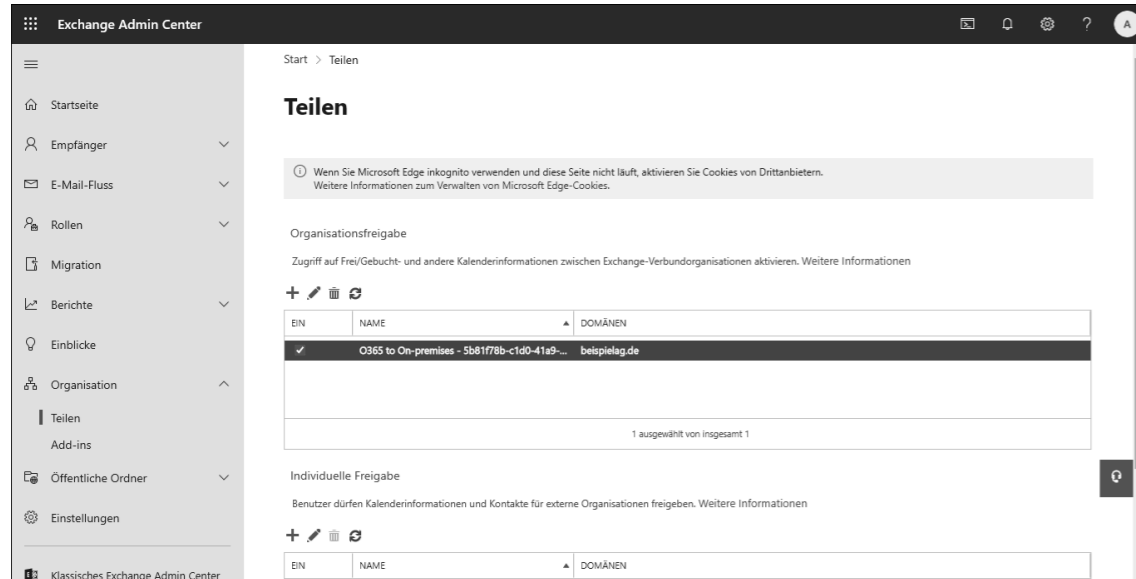


Abbildung 6.162 Konfiguration von Freigaben

Im gleichen Abschnitt finden Sie übrigens die Möglichkeit, Freigaberichtlinien zu konfigurieren. Mit diesen kontrollieren Sie, wie Ihre Anwender Kalender- und Kontaktinformationen an organisationsfremde Personen freigeben können. Welche dieser Richtlinien bei einem bestimmten Postfach Anwendung findet, konfigurieren Sie bei den Postfachfunktionen.

6.11 Migration öffentlicher Ordner

Die Migration von öffentlichen Ordnern einer Exchange-Organisation ist ein recht komplexer Vorgang, der leider nicht über einen grafischen Migrations-Assistenten vorgenommen wird, sondern über eine Reihe von PowerShell-Skripten, die Microsoft zur Verfügung stellt. Bevor wir uns den Skripten zuwenden, möchte ich noch einige Rahmenbedingungen zur Migration erläutern.

Zunächst einmal können Ihre öffentlichen Ordner nur komplett auf einer Seite liegen, also entweder vollständig in Exchange Online oder vollständig in Ihrer lokalen Exchange-Umgebung. Dies betrifft insbesondere eine Hybridkonfiguration (siehe Abschnitt 6.10). Ein Aufteilen der Ordner auf beide Umgebungen ist nicht möglich. Auch müssen bestimmte Voraussetzungen erfüllt sein.